International Standard

ISO 16425

Second edition
2024-01

Ships and marine technology — Specifications for the installation of ship communication networks for shipboard equipment and systems

Navires et technologie maritime — Spécifications pour l'installation de réseaux de communication des navires pour les équipements et systèmes embarqués

Reference number
ISO 16425:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 6, *Navigation and ship operations*.

This second edition cancels and replaces the first edition (ISO 16425:2013), which has been technically revised.

The main changes compared are as follows:

— the title of this document has been changed from “guidelines” to “specification”;

— all Clauses have been revised in line with the shipboard network design procedure;

— designs for Wi-Fi networks, networks equipped with a shipboard data server that conform to ISO 19847 and ISO 19848, and requirements for cybersecurity for shipboard networks have been added;

— in Clause 5, the scope of this document has been included in the network system architecture;

— in Clause 6, information necessary for network design has been provided;

— in Clause 7, the requirements for the operation plan design of the shipboard network have been added;

— in Clause 8, information on shipboard network devices has been added;

— in Clause 9, the network design methods for the physical design of cable and connector for shipboard network equipment and for the logical design of network separation and communication between networks with cyber security have been updated;

— in Clause 10, the equipment, grounding and termination of cables and network equipment have been clarified;

— in Clause 11, network testing and inspection objectives, conditions, methods and criteria have been added;

— in Clause 12, information necessary for network operation has been provided;

— in Clause 13, cyber security requirements for networks have been added;

— in Annex A examples of input/output information required for network design have been added;

— in Annex B, examples of monitoring and managing the shipboard network and the nodes connected to the network have been added;

— in Annex C, an example of secure-network implementation compliant with this document has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document gives specifications relating to communication network-system architecture, data requirements, administration, operation, commissioning, inspection and testing for shipboard equipment and systems.

This document also takes into account differences between shipboard communication networks and networks that are used outside of ships, and stipulates requirements and specifications relating to matters unique to shipboard use.

Until the publication of this document, there has been a lack of comprehensive specifications for connecting devices that are provided by many different manufacturers to a network via a generic means. This gap has impeded the wider use of shipboard networks.

This document aims to improve the convenience for all involved parties, including manufacturers, engineering firms, shipbuilders, and shipping companies.

Ships and marine technology — Specifications for the installation of ship communication networks for shipboard equipment and systems

1 Scope

This document provides installation specifications for ship communication networks, so as to improve communication between shipboard equipment and within shipboard systems that are independent from navigational equipment networks and engine-control networks. This document can also be applied to operational technology (OT) networks that use software and hardware to control and monitor devices and infrastructure such as navigational equipment networks and machinery control networks in ship.

The ship communication networks covered in this document are intended for information sharing and are not directly related to safety of navigation.

This document utilizes existing standards relating to protocols, and provides new specifications for aspects such as communication network-system architecture, administration, operation and installation.

The new specifications in this document include: redundancy, if necessary, for a shipboard communication network system; a network administration that does not require experts; physical as well as logical security; and network installation.

This document uses the standard communication network Internet protocol.

This document applies to shipboard wired networks for IP communication, using Fast Ethernet and Gigabit Ethernet as specified in IEEE 802.3 and to shipboard wireless networks for IP communication, using the unlicensed 2,4 GHz and 5 GHz bands as specified in IEEE 802.11.

NOTE Other wireless technologies based on non-IP communication such as IEEE 802.15.1, IEEE 802.15.4 or wireless communication methods using 920 MHz band are not covered in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 24060:2021, *Ships and marine technology — Ship software logging system for operational technology*

ISO/IEC 11801-1, *Information technology — Generic cabling for customer premises — Part 1: General requirements*

ISO/IEC 14763-3, *Information technology — Implementation and operation of customer premises cabling — Part 3: Testing of optical fibre cabling*

ISO/IEC 20000 (all parts), *Information technology — Service management*

IEC 60092-504:2016, *Electrical installations in ships— Part 504: Automation, control and instrumentation*

IEC 60945, *Maritime navigation and radiocommunication equipment and systems - General requirements - Methods of testing and required test results*

IEC 61162-450, *Maritime navigation and radio communication equipment and systems — Digital interfaces — Part 450: Multiple talkers and multiple listeners — Ethernet interconnection*

IEC 61162-460:2018/AMD1:2020, *Maritime navigation and radio communication equipment and systems — Digital interfaces — Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and security*

IEEE 802.3, *Ethernet (Formerly: Carrier Sense Multiple Access with Collision Detection)*

IEEE 802.11, *Ethernet (Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications)*

ANSI/TIA-568.0:2020, *Generic Telecommunications Cabling for Customer Premises*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
16425-Network
controlled network consisting of devices that meet the requirements of the *16425-Network node* (3.4)

3.2
16425-Network device
hubs (3.21), layer 2 switches, layer 3 switches, routers and other devices that connect and relay between networks

3.3
16425-Network equipment
shipboard equipment for processing, sending and receiving data

3.4
16425-Network node
16425-Network equipment (3.3) and *16425-Network device* (3.2)

3.5
AES
advanced encryption standard
symmetric key cryptosystem

3.6
application level gateway
network infrastructure device that connects 16425-Networks with other networks and which satisfies the safety and security requirements as specified in this document

3.7
business local area network
business LAN
network that crewmembers use for ship operation duties

3.8
broadcast domain
domain on a computer network where broadcasted frames (broadcasts) are received

3.9
collision domain
domain in a computer network where simultaneous transmission cause collisions or congestion

3.10
controlled network
network that has been designed to operate such that authorities are satisfied by documented evidence that the network does not pose any security risks to any connected network nodes

Note 1 to entry: For example, any network compliant to IEC 61162-450 or this document that is approved by classification society, flag state or recognized organization (RO) is considered as a controlled network.

3.11
Crew local area network
Crew LAN
network that crewmembers use for personal matters or in their spare time

3.12
extender connector
non-powered connections, including telecommunication outlets

3.13
data base system
systems equipped on the internet working or shore to manage data efficiently

3.14
DIAMETER
authentication, authorisation, and accounting protocol for computer networks

3.15
DMZ
demilitarized zone
physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and un-trusted network, usually the Internet

3.16
firewall
system installed at network nodes to ensure security by controlling unwanted traffic among different network segments and to and from the internet and other external sources

3.17
gateway
communication device that connects computer networks to networks with differing protocols

3.18
hub
concentrator that is centrally located in a network comprising a star physical topology

3.19
ICMP
internet control message protocol
communication rules that are used for such purposes as notifications of errors in the processing of datagrams, and notifications of information relating to communication

3.20
IP
internet protocol
network layer communications protocol in the Internet protocol suite for relaying datagrams across network boundaries

3.21
IT network
information network not related to onboard control system

3.22
layer 2 switch
hub (3.18) that can direct traffic on an *open systems interconnection reference model* (3.28) layer 2 (data link layer)

3.23
layer 3 switch
hub (3.18) that can direct traffic on an *open systems interconnection reference model* (3.28) layer 3 (network layer)

3.24
log rotation
automated process used in system administration in which log files are compressed, moved (archived), renamed or deleted once they are too old or too big

3.25
MAC address
media access control address
identifier used to identify network interfaces

3.26
MD5
message digest algorithm 5
hash function producing a 128-bit hash value

3.27
MIB
management information base
type of database for managing devices in a network

3.28
OSI reference model
open systems interconnection reference model
model that divides the communication functions for computers into layers

Note 1 to entry: See ISO/IEC 7498 for further details.

3.29
operation technology network
OT network
exclusive network of control and operational technology for optimal operation of products, equipment, and systems on board

3.30
proxy
component acting as an intermediary between two equipment on the network

3.31
port trunk
method of raising transmission speed by governing two or more physical cables

3.32
RADIUS
remote authentication dial-in user service
networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service

3.33
REDS
removable external data source
user removable non-network data source, including, but not limited to, compact discs, memory sticks and devices compliant with IEEE 802.15.1

3.34
SNMP
simple network management protocol
communication rules that define methods for communicating information in order to monitor and control network devices within a network

3.35
shore network
non-shipboard networks, including internet working

3.36
SSID
service set identifier
name which identifies an access point in a wireless network

3.37
SHA
secure hash algorithm
cryptographic hash function

3.38
STP
spanning tree protocol
method of control in a loop topology network for preventing data from entering endless loops

3.39
SYN flood attacks
attack that abuses transmission control protocol (TCP) connections and overloads the system to prevent it from operating

3.40
TAG VLAN
tag virtual local area network
function that adds an ID called a VLAN tag to Ethernet frames to identify the *VLAN* (3.44) to which the frames forwarded across the switch belong

3.41
trouble report
statement reporting the nature of a malfunction to the system integrator, shipowner, or management company, in the event of a malfunction within shipboard equipment or networks

3.42
uncontrolled network
data network that is not compliant with IEC 61162-450, IEC 61162-460, this document, or a controlled network

3.43
UTM
unified threat management
collective control over several different security systems, such as firewall and website filtering, by consolidating them into a single hardware

3.44
VLAN
virtual local area network
method for configuring a local area network virtually, regardless of the physical network configuration

4 Abbreviated terms

AMS	alarm monitoring system
ASCII	American Standard Code for Information Interchange
BR	bridge
BWMS	ballast water management system
C/R	control room
CCR	cargo control room
CD	compact disc
CSMA/CD	carrier sense multiple access/collision detection
DVD	digital versatile disc
ECR	engine control room
E/R	engine room
FBB	fleet broad band
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IP	internet protocol
IT	information technology
LAN	local area network
MAC	Media Access Control
MD5	message digest algorithm 5
MIB	management information base
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
OID	Object Identifier

OSPF	Open Shortest Path First
OT	operational technology
QoS	quality of service
RIP	Routing Information Protocol
RM	room
RSTP	Rapid Spanning Tree Protocol
SHA	secure hash algorithm
STP	shield twisted pair
TCP	transmission control protocol
UDP	user diagram protocol
UTC	Universal time coordinated
UTP	unshield twisted pair
UTM	unified threat management
VDR	voyage data recorder
VDU	visual display unit
VLAN	virtual local area network
VPN	virtual private network
W/H	wheelhouse
WPA	Wi-fi protected access

5 Network system architecture

5.1 Scope of networks system architecture

This network system shall be designed specifically for ships, with the purpose of sharing information between shipboard devices. It shall be independent from navigational equipment networks and engine control networks.

The scope of the network system's architecture is not limited to the bridge. It extends to all key locations on the ship.

The network shall not operate (or control) the ship's navigational equipment, however it is permitted to monitor navigational equipment.

Figure 1 shows a diagram of the network architecture scope in this document. The typical implementation of the contents provided in this document is specified in Annex C. As shipboard networks extend to all important locations onboard ships, the application range of designing, installing, verifying and operating the 16425-network shall not be limited to navigation equipment networks or engine-control networks. If documents prescribe application ranges, these ranges shall be prioritized.

The following are some examples of areas within the scope of the network-system architecture:

— Navigation Bridge/Control Centre;

— Business LAN;

— Crew LAN;

— Server system LAN;

— Engine LAN;

— Field/cargo controller LAN.

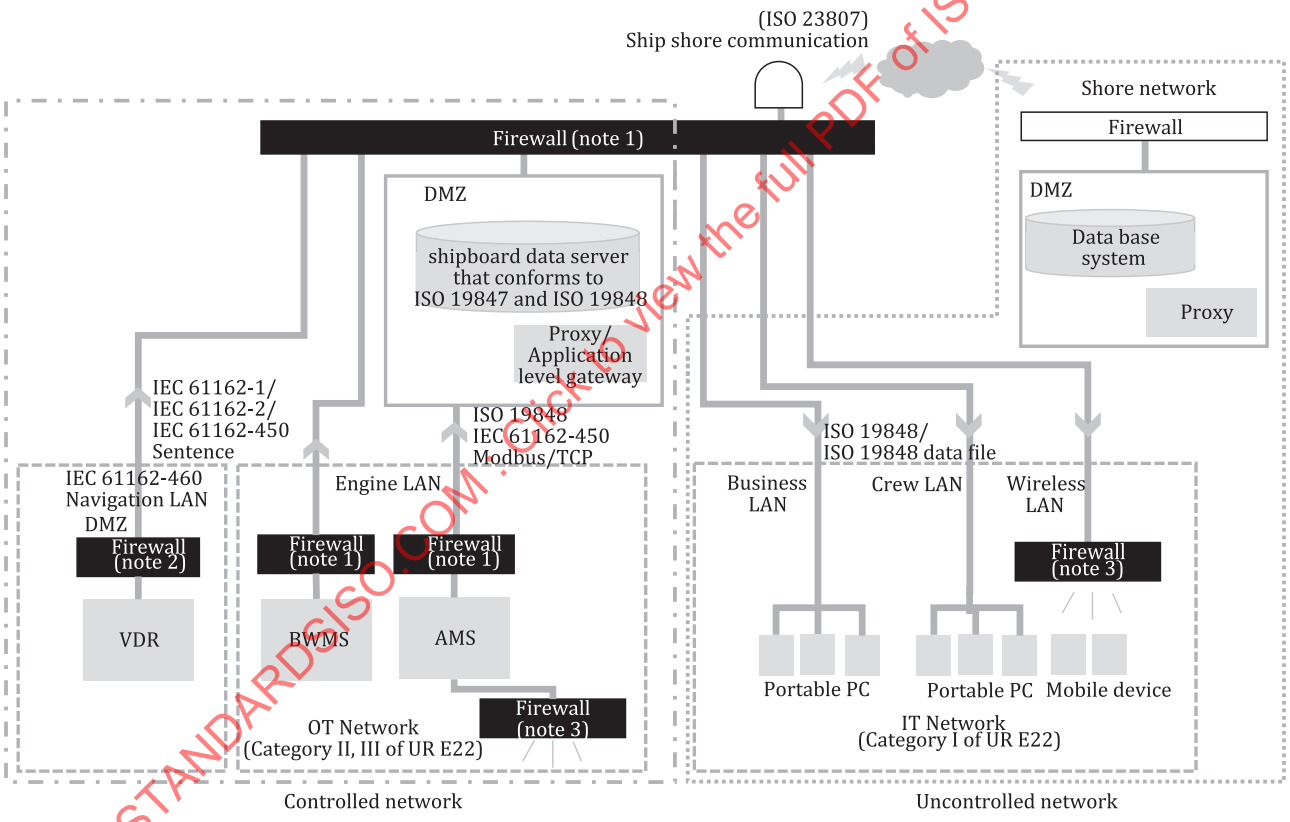
The engine control network and filed/cargo controller network are compliant with this document.

The server system network is configured in the DMZ of an IEC 61162-460 compliant network or an ISO 16425 compliant network.

The Navigation bridge/control centre shall be a network compliant with IEC 61162-450 or IEC 61162-460 that connects to a network compliant with ISO 16425 via a 460-Gateway or 460-forwarder.

Networks compliant with IEC 61162-460 or ISO 16425 are controlled networks. For requirements on controlled networks, see 5.2.

The business LAN and crew LAN are uncontrolled networks.



NOTE 1 The firewall is part of the 460-Gateway or 16425-Gateway. The 16425-Gateway can consist of layer 3 switch, UTM etc.

NOTE 2 The firewall complies with the requirements of the 460-Gateway. The 460-Gateway can consist of layer 3 switch, UTM etc.

NOTE 3 The firewall complies with the 460-Wireless gateway or 16425-Wireless gateway.

Figure 1 — Scope of the network architecture

The functional requirements to use the firewall depend on the capabilities of the network to which it is connected (see Figure 1).

5.2 Controlled network requirements

A controlled network is one that has been designed to operate in such a way that it does not pose any security risks to any of its connected network nodes. This shall, as a minimum, satisfy the following requirements:

— it shall not be possible to connect devices to the network that can be used to insert non-authorized traffic into the network, neither by direct access to the physical infrastructure nor through wireless interfaces;

— network nodes shall not grant a user direct access to operating systems or functions that can be used to insert non-authorized traffic into the network, unless this user is authorized to perform these operations;

— it shall not be possible to transfer data from a non-authorized removable external data source (REDS) or a REDS with un-authorized contents to any node or device in the network.

Most controlled networks also include provisions for hindering non-authorized reading of data in the network, hindering changes in network topology, etc. However, such provisions are not required for the controlled networks that are connected to the 16425-Network.

The system integrator shall provide documented evidence that these requirements are met.

5.3 Network system design

5.3.1 General

The design of this network system shall give due consideration to matters such as the compatibility of the various devices in the network as a whole, and data transmission (amount of information, latency, and routes). Consequently, a network-system designer should have an understanding of the overall system, comprehensive knowledge, and consideration for shipboard use.

When designing the network system, the effective data volume and network load factor should be precalculated when the network media are under maximum load.

When networks are designed, the processes described in Figure 2 shall be followed. In every process, there is information to be input and outcomes to be output, both of which are different from one process to another. Different processes have different conductors to play roles. For the roles of conductors, see 5.4. An example of input and output information required for network design is shown in Annex A.

The squares at the top of the processes listed in Figure 2 represent the information required for the process, and the squares at the bottom of the process represent the deliverables of the process.

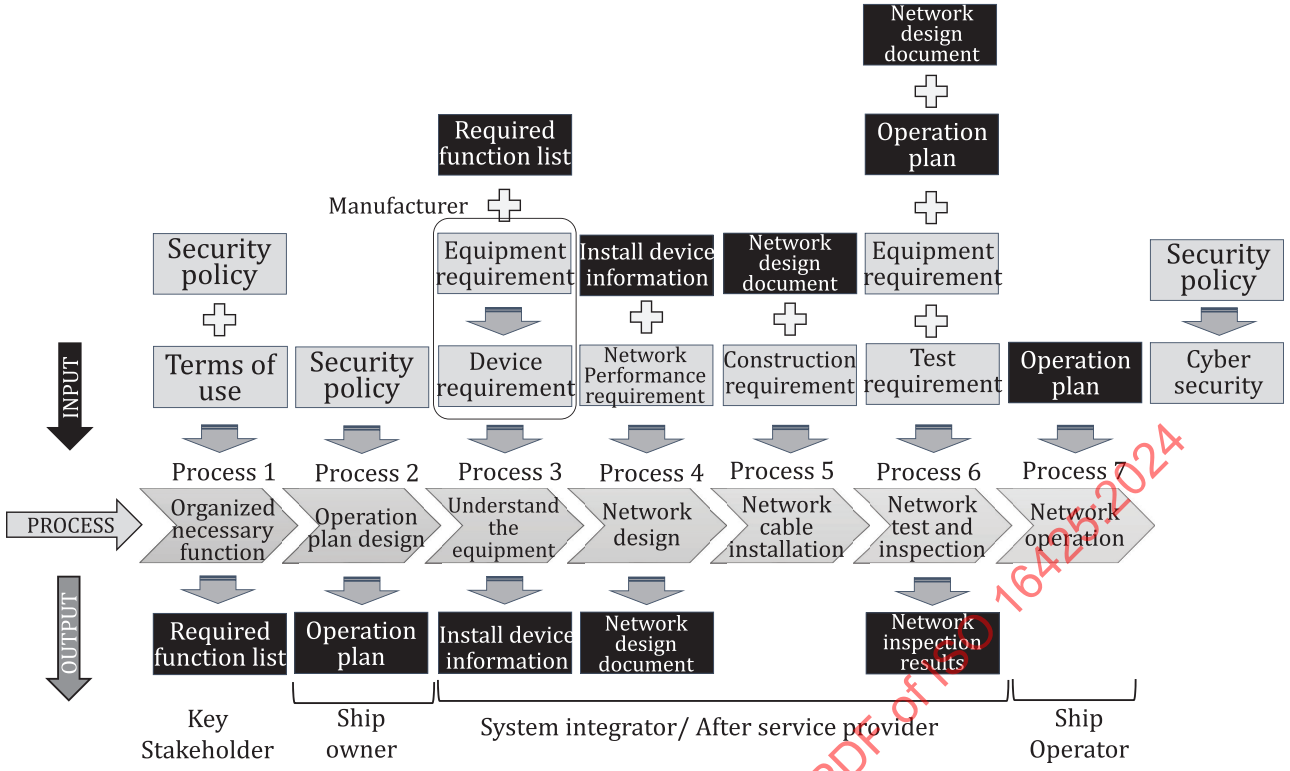


Figure 2 — Shipboard network design processes

5.3.2 Network system separation

The network system shall be separated from other networks by the 16425-Gateway, 460-Gateway or layer 3 switch so that it is not adversely affected by failures on other networks. The routing and filtering rules should be configured appropriately on the 16425-Gateway, 460-Gateway or layer 3 switch for traffic and security. For more advanced security, a firewall for the upper layer can be used.

5.3.3 Network division

The network shall be divided into sub-networks (the broadcast domains) depending on the types of information handled, in order to control traffic and ensure security. Each network should be designed so that network soundness can be maintained at all times, including when failures occur on other sub-networks.

NOTE The following are some examples of sub-networks formed from the main network:

— Navigational data collection sub-network;

— Engine data collection sub-network;

— Shipboard telephone sub-network;

— Imaging sub-network;

— General shipboard document-review sub-network.

5.3.4 Traffic division

The bandwidth used by the core network shall be designed appropriately, and a logical network system shall be built in order to use the network bandwidth more efficiently.

This logical network shall use a virtual local area network (VLAN) architecture, which forms the network from a virtual group that does not depend on the type of physical connections.

During ordinary use, the target traffic on a sub-network should preferably be around 25 % when using half-duplex, and 50 % when using full-duplex communication.

5.3.5 Redundancy

The connections within the network system shall use a redundant architecture that guarantees that information is transmitted without failure. A loop architecture should be used for connections between sub-networks, employing architecture such as a Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) that should act as a spanning tree to quickly route around connection failures.

Using separate routes from the vessel's port and starboard systems for the network's connection cabling is also an effective way to prevent simultaneous network-connection failures.

5.3.6 Cyber security

Shipboard equipment shall be protected from threats from the shipboard networks with which they are connected and the outside network with which the shipboard networks are connected.

5.4 Roles and management

5.4.1 General

Roles apply at various stages of the shipboard network design processes identified in Figure 2. In addition, each role has general requirements that apply to the installation of ship communication networks within shipboard equipment and systems that are specified in this document.

5.4.2 Ship owner

Ship owners shall define functions and specifications for shipboard networks, and policies for designing such functions and specifications. For defining functions, see Clause 6; for designing networks, see Clause 9; and for operating networks, see Clause 12.

5.4.3 System integrator

Based upon the functions, specifications and policies for designing and operating shipboard networks defined by ship owners, system integrators shall choose devices that meet the requirements set forth in Clause 8 to be installed on shipboard networks. In accordance with Clause 9, system integrators shall design shipboard networks and provide ship owners and ship managers with deliverables.

From time to time, system integrators conduct tests for building shipboard networks. In this case, system integrators shall install shipboard network devices and cables in accordance with Clause 10. Thereafter, system integrators shall test and inspect shipboard networks, as prescribed in Clause 11, and submit the results to ship owners and ship managers.

5.4.4 Ship operator

Ship operators shall appropriately run shipboard networks in accordance with policies created by ship owners for running shipboard networks in Clause 12. When there are changes in shipboard network topologies and/or designs resulting from changes in business operations and/or services used, ship operators shall comply with the policies required by ship owners for designing and running necessary functions and shipboard networks. When installing shipboard devices and/or shipboard networks to be used, ship operators shall use products that meet the requirements described in Clause 8. When cables and other equipment are added because networks are expanded or for other reasons, ship operators shall draw designs in accordance with the network design protocols specified in Clause 9 and install 16425-Network devices and wiring in accordance with the Network device and cable installation protocols specified in Clause 10. When needed, ship operators shall conduct tests and inspections on shipboard networks, and keep documents on shipboard network designs, as specified in Clause 11.

5.4.5 Manufacturer

Manufacturers provide devices used with shipboard networks, 16425-Network devices and 16425-Network equipment. The devices used for shipboard networks, 16425-Network devices and 16425-Network equipment that manufacturers provide shall comply with the requirements set forth in Clause 8. When requests are made by ship owners, ship operators and/or system integrators to provide protocols and/or traffic, manufacturers shall comply with such requests.

NOTE When information is provided, confidential agreements are signed in some cases between/among ship owners, ship operators, system integrators and manufacturers.

5.4.6 After-sales-service provider

When making changes of shipboard network topologies and/or renewing devices that are used with shipboard networks and/or 16425-Network devices at the request of ship owners or ship operators, after-sales-service providers shall comply to meet functions and specifications defined by ship owners and policies for designing and operating shipboard networks defined by ship owners. Shipboard devices and 16425-Network devices used shall be products meeting the requirements set forth in Clause 8.

When cables and other equipment are added because networks are expanded or for other reasons, ship operators shall draw designs in accordance with Clause 9 and install 16425-Network devices and wiring in accordance with Clause 10. When needed, ship operators shall conduct tests and inspections on shipboard networks, as prescribed in Clause 11. After-sales-service providers shall, then, submit reports to ship owners or ship operators regarding changes made, dates on which the changes are made and test results, and have them reflected on documents on designing shipboard networks.

6 Organized necessary function

6.1 General

Ship owners shall clarify the purposes of building shipboard networks, and define what information is required to accomplish these purposes.

6.2 Necessary information

Ship owners shall submit information on the following items to system integrators.

a) services used on shipboard networks;

b) parties using such services;

c) down time to be tolerated in such services (targeted operation rates);

d) applications required to enjoy such services;

e) information (data) required to enjoy such services;

f) new risks;

g) parties (equipment) that have necessary information;

h) locations of such parties (equipment);

i) plans for expansions after ships are deployed in service;

j) clarification of cybersecurity management systems and policies;

k) operation plan design;

l) security policy.

Security policies are not applied exclusively on board but should be applied to all relevant organizations, including ships.

7 Operation plan design

7.1 General

System integrators shall design plans for operating shipboard networks in accordance with organized necessary functions defined by ship owners (see Clause 6). Designing plans for operating shipboard networks is important to safely continue to operate shipboard networks.

In operation plan design management, the specific items and contents to be monitored, maintenance details, backup and log management methods, and reporting operations should be based on the ISO/IEC 20000 series.

For items to manage, see 7.3.

7.2 Objectives for managing shipboard network operations

System integrators shall submit operation plans to ship owners when they are designed. By managing shipboard network operations, the objectives described in Table 1 and a) to f) below can be achieved.

Table 1 — Objectives for managing shipboard network operation

Shipboard network operations	Advantages	Functions					
		Configuration management	Fault management	Performance management	Cost management	Security management	Operation support
Efficient operations	Appropriate use of shipboard network resources	Yes		Yes			
	Easy use of shipboard network states	Yes	Yes	Yes	Yes		Yes
Easy operations	Temporarily separate faults from machinery			Yes			
	Minimize function losses when there are failures	Yes	Yes	Yes			
	Quickly see how much failures spread		Yes				
	Easily add shipboard networks/ make configuration changes in integrated fashions	Yes					Yes
	Easily see shipboard network operations (performances)			Yes			
Safe operations	Fully accomplish system security					Yes	
Fault countermeasures	Easily separate failures in early stages (at node levels)		Yes				
Preventive maintenance	Easily conduct repair/ replacement work	Yes	Yes				

The following is an elaborated list of the outcomes in Table 1.

a) Configuration management

Information on shipboard network routes (logical and physical paths), node connections and configurations and operation control are maintained and managed, and operating states are monitored and transmitted.

b) Failure management

By determining and reporting failures that can occur at nodes in shipboard networks, diagnosing the failures, making operation checks and reporting results and taking actions planned in accordance with the failures, it is easier to separate failed areas at early stages, project how much of the failure will spread, and take precautionary and maintenance actions.

c) Performance management

By statistically tallying and appropriately evaluating shipboard network operations, such as traffic and response time, it is possible to efficiently use network resources and draw appropriate plans for expansion work.

d) Cost management

By managing data traffic, it is possible to appropriately manage costs regardless of whether communication is performed under the pay-as-you-go system or at fixed rates.

e) Security management

Security is supported for communications between nodes connected with shipboard networks.

f) Operation support

Different from configuration and failure management, operation support enables networks to be operated and managed smoothly at application levels.

7.3 Items to manage

7.3.1 Items to manage devices and cables to be installed

Devices, cables and codes to be installed shall be managed on lists. Lists shall contain dates when they were created and updated, and information on different versions.

7.3.2 Items to monitor and details

To operate shipboard networks, the state of shipboard network resources for 16425-Network devices and resources for shipboard equipment shall be monitored.

7.3.3 Details of maintenance

Rules shall be established for applying patches, approving and performing upgrading work, controlling access, making setting changes and carrying out machinery maintenance.

7.3.4 Back-ups and log management

Rules shall be established for data and logs, in terms of back-ups, replacement, media storage, rotation, monitoring and compressing.

7.3.5 Operation of reports

Rules shall be established for regular and trouble reports.

7.3.6 Service management

Rules shall be established for managing incidents in accordance with the ISO/IEC 20000 series.

8 Understanding the equipment to be installed

8.1 Understanding the equipment

8.1.1 General

Equipment to be installed on shipboard networks shall meet the requirements specified in 8.2. System integrators shall document the protocol and traffic information shown in 8.3 and the information required for the design of the shipboard network shown in 9.8, regarding the equipment installed on the shipboard networks.

This document shall be kept as an inventory list and updated during the construction and operation of the ship. Hardware and software information should be updated to ensure that new vulnerabilities and dependencies are not introduced and are handled appropriately to reduce the risk.

8.1.2 Inventory lists

In order to understand the information of the connected equipment, it is necessary to summarize the information related to communication, such as the protocol and data format of the equipment, required cable type, required data and transmitted data, installation location, understanding of the status monitoring function of the equipment, importance of the application, requirements for redundancy, and communication volume. It is also necessary to understand the location of the device and what kind of network topology is required for the device, as well as to summarize prohibited items (items that cannot be handled by security policies or devices) and restrictions rather than necessary functions.

Information on these hardware and software versions shall be maintained in inventory lists (see 12.2.2.1).

8.2 Requirements for the 16425-Network device and 16425-equipment installed in the shipboard network

8.2.1 General cyber security requirements for 16425-Network devices and 16425-equipment

8.2.1.1 REDS security

For removable external data source security, refer to IEC 61162-460:2018/AMD1:2020, 6.2.3.

8.2.1.2 Access control

If the equipment has the capability for software maintenance by crew or service personnel, the equipment shall have a mechanism to identify and authorize users to restrict operation and use of resources. Appropriate authorization shall be assigned to the user and only operations and use of resources consistent with the authorization shall be permitted.

The device shall have at least two authorizations to restrict its operation: general user and administrator with maintenance mode. The identification of the user is carried out by means of an identification and password, through an account, or by means of a physical key authorization. In the case of multi-factor authentication, a combination of these is used, or otherwise. It shall be possible to restrict the operation of the system by using tools that are restricted to service personnel.

8.2.1.3 User authentication

If user identification is by means of an identification and password, a) to e) shall be met.

If password-based user authentication is used, a) to e) shall also be met, except that additional password restrictions may be enforced by the manufacturer, such as password length, character complexity, excluded word lists, etc.

a) Passwords shall be case-sensitive.

b) Administrator passwords shall be at least 10 characters long and contain a combination of at least three (3) of the following: numbers, uppercase and lowercase letters, and special characters.

c) Passwords for ordinary users shall be at least eight (8) characters in length and shall be a combination of at least two types of alphanumeric and special characters: numbers, uppercase and lowercase letters and special characters.

d) The password shall be a random and meaningless password, not a word found in a dictionary.

e) Passwords shall be strictly stored and managed so that they are hidden from unauthorised persons.

8.2.2 Network interface for 16425-Network equipment and 16425-Network device

8.2.2.1 General

Requirements are defined for devices which are equipped with shipboard networks and shipboard network devices.

8.2.2.2 Interface

The 16425-Network shall use the local area network specified in IEEE 802.3 that is most frequently used for computer networks, and a wireless network specified in IEEE 802.11.

8.2.2.3 Connected equipment

The devices to be connected to the 16425-Network shall be 16425-Network devices that shall share information onboard the vessel.

8.2.3 Requirements for 16425-Network nodes

8.2.3.1 General

The nodes connected to the ship network are classified according to the degree of impact on the ship in the event of a failure. Classifications are called system categories (see Table 2), and the requirements for the 16425-Network node vary by system category.

Table 2 — System categories

Category	Failure effects	Typical system functionality
I	Those systems, failure of which does not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	Monitoring function for informational/ administrative tasks
II	Those systems, failure of which can eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	— Alarm and monitoring functions — Control functions which are necessary to maintain the ship in its normal operational and habitable conditions
III	Those systems, failure of which can immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	— Control functions for maintaining the vessel's propulsion and steering — Vessel safety functions

8.2.3.2 16425-Network nodes (Category I, Category II and Category III)

8.2.3.2.1 16425-Network nodes function requirements

Category II/III equipment installed in the 16425-Network shall meet the requirements a) to g).

a) Category II/III equipment installed in the 16425-Network shall be capable of providing one of the management functions set forth in B.1.2.1.

b) Category II/III equipment installed in the 16425-Network shall be able to control the use of mobile codes.

   When normal operations cannot be maintained, the equipment shall be able to either limit the use of the latest known values or fixed values, as described in manufacturers' instruction manuals.

c) Category II/III equipment installed in the 16425-Network shall provide the function to limit the use of automatic release resources so as not to exhaust CPUs, memory, storage and other resources.

d) Category II/III equipment installed in the 16425-Network shall provide the function to collect definition information that affects system operations and back up saved information without impacting normal operations.

e) Category II/III equipment installed in the 16425-Network shall provide the function to resume a known protected state in case such a state is lost due to breakdowns and other accidents.

f) Category II/III equipment installed in the 16425-Network shall not lose essential services or functions even if there are audit process failures.

g) Category II/III equipment installed in the 16425-Network shall take actions to prevent falsification of checksums or other tools when communication is made between 16425-Network equipment.

8.2.3.2.2 16425-Network nodes management information

16425-Network nodes shall provide information in response to requests from the network monitoring function.

See 8.2.4.6 for the network monitoring function.

8.2.3.2.3 16425-Network nodes functional safety general

16425-network nodes should comply with functional safety standards (e.g. the IEC 61508 series).

Cyber security function should not adversely affect the essential functions or functional safety of ISO 16425-network nodes. If there is a conflict between the functional safety function and the cyber security function, the functional safety function shall be performed prior to the cyber security function and shall provide evidence of 16425-Network nodes.

8.2.4 Requirements for 16425-Network devices

8.2.4.1 General

Devices intended to be connected with the 16425-Network shall meet the requirements specified in 8.2.4.2 to 8.2.4.5.

8.2.4.2 Device constituting communication network system

8.2.4.2.1 Device access control

Changes in network switch, network 16425-Gateway and 16425-Wireless Gateway configurations require authentication from users.

For more information on device access control, see 13.1.4.

8.2.4.2.2 Traffic prioritization

The 16425-Gateway and 16425-Wireless Gateway may prioritize some or all of the traffic from the 16425-Network to the other controlled and uncontrolled networks.

8.2.4.2.3 16425-Network device function requirements

The 16425-Network device function shall be able to define network flows with combinations of interfaces, MAC addresses and IP addresses, protocol numbers and TCP or UDP port numbers.

All unregistered network flows are prohibited.

If VLANs are provided, it should be possible to configure VLANs on a per-interface basis and to support the VLAN protocol version specified in IEEE 802.1Q:2018 (TAG VLAN).

Loop prevention functions such as RSTP and MSTP shall be provided.

NOTE Loops can be produced by misconfigurations. They can also be generated when there are multiple passes due to network topologies or network redundancies.

The 16425-Network device function supports at least the RSTP protocol version of IEEE 802.1s-2002.

Layer 2 switch, layer 3 switch and firewall shall provide the function to make RSTP effective on all interfaces.

8.2.4.3 16425-Gateway/16425-Wireless Gateway

8.2.4.3.1 Requirements

The 16425-Gateway and 16425-Wireless gateway shall meet the following requirements or the requirements for the 460-Gateway set forth in IEC 61162-460:2018, AMD1:2020, 6.3.5.

The following requirements in a) to f) apply to IP communication on controlled and uncontrolled networks.

a) For connections from uncontrolled networks, “not allowed” shall be set as the default.

b) Inward and outward firewalls shall be provided, consisting of source and destination IP addresses, protocols and port numbers.

c) Lists shall be provided of conditions for all direct connections between controlled networks and uncontrolled networks.

d) Lists shall be recorded in the 16425-Gateway and 16425-Wireless gateway or external devices, which shall include changes made in the last 12 months.

e) A list of lists shall be available.

f) Information on source and destination IP addresses, connection start and termination time and TCP port numbers shall be recorded whenever direct connections are made.

8.2.4.3.2 Management functions

8.2.4.3.2.1 General

Network nodes shall provide information in response to requests from network monitoring function.

The 16425-Gateway and 16425-Wireless gateway shall have the following functions:

a) Maintain the configuration information (Config) of all network infrastructure and be able to restore it when requested.

b) The management function shall maintain at least a history of previous configurations.

c) Save and restore configuration information automatically or manually.

d) Change the configuration information of the network infrastructure.

8.2.4.3.2.2 Network traffic control

Functions shall have been provided to protect networks from Denial of Service (DoS) attacks.

NOTE Some network switches provide protection functions alone, but such products are limited. They are, as such, not a realistic option. It is more realistic to adopt dedicated and other devices. Ways can be provided to prevent Distributed Denial of Service attack (DDoS) or Distributed Reflective Denial of Service (DRDoS) attacks.

8.2.4.3.2.3 Management information

The 16425-Gateway and 16425-Wireless gateway shall provide information in response to requests from network monitoring function.

See 8.2.4.6 for the network monitoring function.

8.2.4.3.2.4 Filter conditions

Authorization conditions can be registered for all connections between controlled and uncontrolled networks.

Authorization conditions can also be registered for all connections between the controlled network or uncontrolled network and the DMZ.

The 16425-Gateway and 166425-Wireless gateway shall have a filter function to restrict the input and output of data to the interface at three or more open systems interconnection (OSI) reference model layers.

The restriction shall be able to be applied to both input and output.

The filter function of the 16425-Gateway and 16425-Wireless gateway shall have the following functions:

— maintain configuration information and be able to restore it when requested;

— maintain a history of previous configurations;

— save and restore settings automatically or manually.

8.2.4.3.2.5 Access via un-controlled network

The system shall be provided the capability to monitor and control all methods of access to the equipment via uncontrolled networks.

8.2.4.4 16425-Wireless gateway

8.2.4.4.1 Function requirement

8.2.4.4.1.1 Frequency requirements

The 16425-Wireless gateway shall be able to use both 2,4 GHz and 5 GHz frequencies and shall be able to emit radio waves at the same time as one or the other.

8.2.4.4.1.2 Authentication method

To ensure the security of the wireless LAN, both WPA3 personal and WPA2 personal authentication methods shall be available.

The MAC address authentication function shall be available.

8.2.4.4.1.3 Encryption

The encryption shall be able to use Advanced Encryption Standard (AES).

8.2.4.4.2 Use control for portable and mobile device

Portable PCs and mobile devices to be linked with the 16425-Wireless gateway shall be protected from the risks of malware infections and information leakage.

8.2.4.5 Layer 2 switch/layer 3 switch/firewall

Layer 2 switches, layer 3 switches and firewalls used in category II and category III systems shall have the following capabilities:

— maintain all network infrastructure configuration information (Config) and be able to restore it when requested;

— maintain a history of previous configurations;

— save and restore network infrastructure configuration information automatically or manually;

— provide the information required by the network monitoring function.

8.2.4.6 Network monitoring function

8.2.4.6.1 Network monitoring function requirements

The network monitoring function monitors the load, redundancy, and topology of the network and assists the operation and maintenance of the network by generating alerts. The network monitoring function shall be available at least on the devices installed in the 16425-Network.

The network monitoring function shall be provided a human-machine interface (HMI).

The network monitoring function shall be recorded and retain alerts and events as required.

Alerts from the network monitoring function are events from 16425-Gateway, 16425-Wireless gateway, layer 2 switches, layer 3 switches, firewalls, from nodes that can provide Management Information Base (MIB) upon request via Simple Network Management Protocol (SNMP), or reports triggered by the network monitoring function.

The records shall be able to be displayed in a format suitable for the user to review.

The network monitoring function should have the function to either automatically or manually save and restore 16425-Gateway and 16425-Wireless gateway configuration information.

The network system management function may have redundancy.

8.2.4.6.2 Network load monitoring function

The system documentation shall include the maximum traffic that the manufacturer-declared system sends to the 16425-Network. The network load monitoring function shall constantly monitor the network load so that the load does not exceed 80 % of the link speed.

8.2.4.6.3 Redundancy monitoring function

The system documentation shall include a list of data sources that are redundant by either cable redundancy, interface redundancy or device redundancy.

The Interface redundancy list contains the MAC addresses of the interfaces to which the 16425-Gateway, 16425-Wireless gateway, layer 2 switch, layer 3 switch and firewall are equipped. If the IP address and Service Set Identifier (SSID) are the same due to redundancy, the list of device redundancy includes the MAC address of each device used for redundancy so that it can be uniquely identified.

8.2.4.6.4 Network topology monitoring function

The system documentation shall include a list of the MAC addresses of the interfaces that are connected to the devices equipped with the 16425-Network.

The network monitoring should be available at least on the devices installed in the 16425-Network.

In order to maintain the network topology, changes in the network topology shall be monitored.

The network topology monitoring function shall use SNMP and require network configuration information at least every 30 minutes from 16425-Gateway, 16425-Wireless gateway, layer 2 switch, layer 3 switch, router and firewall.

If there is a MAC address found that is not included in the system documentation, the network topology monitor shall generate an alert.

As an example, the requirements for network topology monitoring are described in Annex B.

8.2.4.6.5 Management devices

The network monitoring equipment shall monitor the health and interface status of the 16425-Gateway, the 16425-Wireless gateway, the layer 2 switches, layer 3 switches and firewalls that make up the category II/III systems in Table 2.

Layer 2 switches, layer 3 switches and firewalls used in category I nodes and systems in Table 2 should be monitored for health and interface status (see 8.2.4.5).

The status of the interfaces refers to at least the following items.

a) Power loss of active (powered) 16425-Network device

b) Link speed

c) Differences between half- and full-duplex communication

d) Link up and down

e) Traffic (data amounts)

f) RSTP (MSTP) mode (if the device is equipped with it)

g) Loop detect status (if the device is equipped with it)

8.2.4.6.6 Management equipment

The network monitoring equipment may monitor the health of the equipment fitted within the 16425-Network and the status of the interfaces, which includes at least the following information.

a) Power loss of active (powered) 16425-Network node

b) Link speed

c) Differences between half- and full-duplex transmission

d) Link up and down

e) Traffic (data amounts)

8.2.4.6.7 Log recording function

The 16425-Gateway and the 16425-Wireless gateway in the 16425-Network, as well as the layer 2 switches, layer 3 switches and firewalls comprising the category II/III systems in Table 2, shall be able to log and display logs.

NOTE The device which constitutes category I of Table 2 can be provided with log recording and display function.

8.3 Protocol and traffic

8.3.1 General

When devices installed on board ships communicate with other nodes through shipboard networks, system integrators shall have an understanding of the protocols and traffic to communicate, and the types of cables used in the categories.

8.3.2 Protocol

As for communication protocols, it is necessary to understand protocol types (TCP/IP, UDP uni-cast, UDP multicast and UDP broadcast), communication directions and the port number.

There are two types of port numbers: source port and destination port. It is necessary to confirm both port numbers and whether the settings can be changed.

8.3.3 Traffic

It is necessary to understand the maximum traffic and the when maximum traffic can occur.

8.3.4 IP address

As for IP addresses, it is necessary to understanding whether static or dynamic addresses are supported, whether the settings can be changed, and whether the default gateway address can be set.

8.3.5 MAC address

It is necessary to understand MAC address.

8.4 Cable

8.4.1 General

It is necessary to understand the categories of cables used for devices that shall be connected with networks. It is also necessary to understand if shields are required and how to lay cables.

8.4.2 Cable specification

It is necessary to understand the categories of cables required by the devices and the specifications of the cables to be used. Categories of cables are classified in terms of the different temperatures at which they can be used, and the maximum lengths to achieve their best performance.

8.4.3 Cable earth method

Cables are categorised into two types: shielded cables (STP) and unshielded cables (UTP). It is necessary to see whether shields are needed. In the case of STP, the installation can be different, depending on the devices with which the cables are connected. It is necessary to know whether both ends of the cables are connected or only one end.

9 Network design

9.1 General

In designing shipboard networks, it is necessary to fully consider compatibility among various devices in entire networks and various factors relating to data transmission (i.e. information quantities, latency times and routes). Shipboard network system designers shall organize entire networks and have extensive knowledge and understanding of the networks used on board ships.

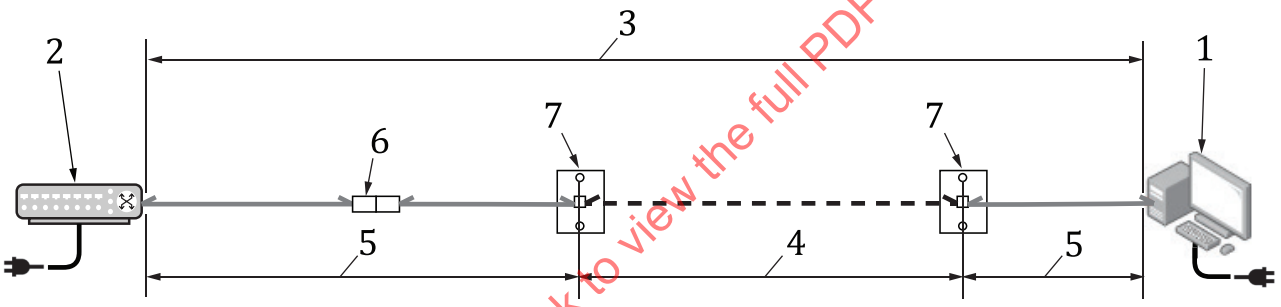
In designing shipboard networks, it is necessary to calculate valid data amounts in advance and network load factors at the time of the maximum network load. It is also necessary to consider shipboard network expansions and data traffic increases.

To define what means of communication are allowed in various failure scenarios, including security incidents, designs shall be drawn in anticipation of various system states, including initial, failure and normal states.

9.2 Concept of shipboard network system

9.2.1 General arrangement

A shipboard network system is composed of a combination of the network subsystems. A network subsystem comprises the components described in Figure 3.



Key

1 network node
2 network device
3 channel
4 permanent lnk
5 code
6 extender connector
7 telecommunication outlet

Figure 3 — Network subsystem

9.2.2 Channel

A channel is a transmission path between a 16425-Network device, such as a layer 2 switch, and a network node, such as a server.

9.2.3 Permanent ink

A permanent link is a fixed, laid Ethernet cable in the channel.

9.2.4 Code

The code is a movable ethernet cable used for connecting the jack to the end of the 16425-Network device/16425-Network equipment.

9.2.5 Extender connector

The extender connector is a passive (non-powered) component that connects two ethernet cables for extending the cable length or for other purposes.

9.2.6 Telecommunications outlet

The telecommunications outlet is a passive (non-powered) component that connects two ethernet cables for extending the cable length or for other purposes.

The telecommunications outlet is mounted on walls or other surfaces for easy connection to network nodes.

9.3 Design standard

9.3.1 Category of cables and codes

The categories of cables and codes (e.g. category 5E or category 6), shall be clarified in network design documents (see 9.8.1).

9.3.2 Plug connection method

The methods of plug connections, e.g. TIA/EIA-568-A or TIA/EIA-568-B.1 shall be clarified in network design documents (see 9.8.1).

9.3.3 Specifications for naming cable

Each cable shall have identification marks, such as cable names, marks and cable colours. When extended with repeaters/extender connectors, each cable shall have identification marks to indicate the channels to which they belong. Specifications for giving identification marks shall be clarified in network design documents (see 9.8.1).

9.3.4 Model number of cable, code, plug, jack and crimping tools to be used

The model numbers and manufacturers of all cables, codes, plugs, jacks and crimping tools to be used with and for networks shall be clarified in the network design documents (see 9.8.1).

9.4 Physical design

9.4.1 Selection of 16425-Network equipment

9.4.1.1 General requirement

16425-Network equipment shall be selected to withstand environmental conditions (temperature, humidity, changes in temperature and humidity, corrosive and/or volatile gases oil-contained air, dust and electromagnetic factors) in the location they are installed.

As for temperature, equipment generates heat itself, raising surrounding temperatures. As such, equipment that can work at higher temperatures shall be selected.

9.4.1.2 Metal cable, plug and jack

All cables, plugs and jacks used in a network should be of the same category.

NOTE If a network contains cables, plugs and jacks of different categories, the network is regarded as having cables, plugs and jacks of the lowest category of the three.

All cables on a ship should be straight cables.

Single-wire cables shall be used.

The appropriate plugs and crimping tool shall be adopted, depending on the core wires (single or stranded), outer diameter shields and make of the plugs.

9.4.1.3 Code

Stranded-wire cables may be used for the code. However, stranded-wire cables longer than 10 meters shall not be used.

Even if an STP cable is used for the permanent link, UTP codes may be used for the code.

9.4.1.4 Extender connector and telecommunications outlet

For UTP cables, UTP extender connectors shall be used. For STP cables, STP extender connectors shall be used. Up to four extender connectors or telecommunication outlets shall be used for a single channel. When telecommunication outlets are used, codes measuring up to 10 m are connected. As such, cables shall be reduced in length accordingly (cables shall be shortened by 10 m when codes are connected on one end, and by 20 m when they are connected on both ends).

9.4.1.5 Repeater/repeater hub

Repeaters and repeater hubs shall not be used for any other purpose than maintenance and debugging.

They shall not be used to extend cables length (cable length extensions cannot be made with repeaters or repeater hubs).

NOTE Repeaters and repeater hubs cannot separate collision domains.

9.4.1.6 Layer 2 switch

Layer 2 switch shall have the monitoring functions described in 8.2.4.5.

Layer 2 switches that have VLAN functions may be used to isolate networks logically.

9.4.1.7 Layer 3 switch/router

Layer 3 switches and routers shall have the monitoring functions described in 8.2.4.5.

Layer 3 switches and routers are devices with very similar roles, to sort the destination of packets at layer 3. When used exclusively for this purpose, both layer 3 switches and routers are available. Choices can be made between them, depending on other the functions and specifications that they have.

Layer 3 switches and routers should not be used for network isolations. Networks that are connected to each other with layer 3 switches and/or routers at layer 3 without having firewalls cannot block communication among the networks; as such, they are regarded as belonging to the same network.

When routing among networks is not performed, layer 3 switches and routers may be used for network isolation. In that case, physical isolation shall be considered instead of using layer 3 switches or routes (to avoid risks in case layer 3 switches and/or routers are overtaken by third parties).

NOTE VLANs are layer 2 protocols.

9.4.1.8 Firewall

Firewalls are used to block communication among networks.

The firewalls shall have the monitoring functions described in 8.2.4.5.

The firewalls shall block all communications among networks except for approved ports, protocols and services.

9.4.2 Cabling

9.4.2.1 Cable route

Cable lengths shall not exceed 100 m (in case of metal cables). Even when extended with extender connectors or repeaters, total lengths that include extensions shall not exceed 100 m.

When cables are used with codes, cable lengths shall not exceed 90 m.

In case of redundancy, different routes should be taken.

The route should be separated from electrical lines such as those for the motor power and lighting. When it is difficult to separate routes, shielded cables shall be used and appropriately installed in accordance with installation standards.

Shortening of cables to their maximum lengths shall consider a rise in temperature from nearby power lines and other factors, and appropriate cable lengths shall be kept in accordance with the temperatures in areas surrounding cable routes.

9.4.2.2 Extender connector (passive, non-powered)

Extender connectors shall not exceed four tiers. Tests shall be conducted between end connectors that have extender connectors between them.

9.4.2.3 Protection

Steel braided armoured cables shall be used on all occasions except when cables are laid indoors and/or in enclosure.

When cables are laid in hidden spaces, such as behind walls, steel braided armoured cables shall be used.

9.4.2.4 Use of optical fibre

When extending cables, consider the use of layer 2 switches first.

When it is impossible to extend cable length with layer 2 switches, optical fibres may be used.

If this is the case, take into consideration that even very minute grit, dust and flaws on an optical fibre connector end surface, measuring as much as several micrometres in size, can have an adverse impact on signals. This can generate a risk of melting and causing other damage to the connector ends.

9.4.2.5 Use of PoE

Power over Ethernet (PoE) devices shall be protected from unintentional cable disconnection by the user. Plugging and unplugging PoE live cables can cause damage to devices.

The cable length shall be determined by taking into account the reduction in cable length due to the heat generated by the PoE cable itself.

When receiving power from PoE, make sure that the total quantity of power from power supply hubs does not exceed the hubs' PoE supply capacities. Also ensure that the quantity of power used by PoE devices does not exceed the supply capacity at each port of power supply hubs. When the quantity of power used is

calculated, it is necessary to consider that 2,5 watts are lost when the quantity of power used is 16 watts or less, and 6 watts are lost when it exceeds 16 watts.

When receiving power from PoE, cables of category 5E or higher shall be used.

9.4.3 Separation of collision domain

Collision domains shall be separated per single channels by layer 2 or higher devices. In other words, repeater hubs shall not be used in actual operating situations.

NOTE Collision domain separation does not affect broadcast or multicast domains.

9.4.4 Setting of interfaces

Transmission parameters at both ends of collision domains shall be of the same configuration. When auto negotiations are used, they shall be applied to both ends.

9.4.5 Installation

16425-Network equipment shall be fixed. In other words, their weight shall not be supported by other network equipment (e.g. extender connectors that are not fixed on boards or walls but supported by cables).

16425-Network equipment other than cables and codes shall be protected so that only authorized users can operate them (e.g. boards with keys and locks).

9.5 Logical design

9.5.1 General

To ensure security and stability, shipboard networks shall be designed to minimize mutual interference between networks by separating networks physically, or logically with VLANs.

9.5.2 Isolation of network

9.5.2.1 Class of network

Networks are roughly classified into the following four classes:

— OT networks;

— business LAN;

— welfare networks (networks that can be accessed with crewmembers' personal devices);

— DMZs.

Networks are groups of sub-networks where inputs and outputs are managed so that mutual communication is controlled. In addition, the OT network shall be segmented on a per-system basis. For network segmentation, see 13.1.6.1.4.

9.5.2.2 Internetworking communication

Direct communication from internetworking to the controlled network shall be denied in principle. Welfare networks shall be allowed to communicate exclusively with DMZs. However, in this case the ports, protocols and services shall be controlled so that only a minimum level of communication is allowed.

When communication is allowed between OT networks and/or between OT and business networks, close attention shall be paid to contents and volumes. Communication between parties shall be held down to necessary bare minimum ports, protocols and services (PPS), and contents and volumes shall be fully controlled.

9.5.3 Broadcast domain

9.5.3.1 Separation of broadcast packet

Shipboard networks shall be designed to minimize broadcast domains.

A broadcast domain is a network that is reachable by broadcast packets. Broadcast domains are separated by routers and other layer 3 switch or higher devices. Broadcast packets do not move beyond broadcast domains, but attention shall be paid as it is possible to send broadcast packets to other domains (for directed broadcast, broadcast packets are not sent to original domains).

9.5.3.2 Network address

Excessively extensive address space shall not be designed (spare addresses shall be minimized).

9.6 Reliability design

9.6.1 General

Depending on the reliability levels required for shipboard networks, a redundant network may be required. To meet such demands, shipboard networks shall be designed so that cables/codes and 16425-Network equipment can both be redundant to eliminate single faults, and that abnormalities can be corrected immediately by monitoring shipboard networks.

9.6.2 Redundancy

9.6.2.1 Redundancy of cables with RSTP (MSTP)

When RSTPs (MSTP) are used, loop detectors and storm guards shall both be activated.

Blocking port locations shall be detected and indicated.

When there is a single disconnection (where all communications on the network are still functioning), the locations of the disconnections shall be detected.

9.6.2.2 Redundancy of network nodes

Redundant network nodes (servers and others) shall not be connected with the same 16425-Network devices (switches and others).

9.6.3 Monitoring of shipboard networks

9.6.3.1 Monitoring of 16425-Network device interfaces

The existence of active (powered) 16425-Network devices shall be confirmed with ICMP or SNMP.

9.6.3.2 Monitoring of topology changes

When large volume communication is established on a regular basis, decreases in link speed and changes from full to half duplexes should be monitored and notified. Necessary communication can be disrupted.

9.6.3.3 Monitoring of shipboard network status

At least the following items should be monitored at 16425-Network devices and/or 16425-Network network nodes, which are connected to the network.

a) Network load (16425-Network devices and/or 16425-Network equipment)

b) Link speed (16425-Network devices and/or 16425-Network equipment)

c) Link up/down (16425-Network devices)

d) RSTP (MSTP) mode (16425-Network devices, if applicable)

e) Loop detect status (16425-Network devices, if applicable)

9.6.4 Load design

Shipboard networks shall be designed so that packet collisions do not occur.

Shipboard networks shall be divided appropriately to split broadcast domains (the domains reached by broadcasts), and to ensure that the repeater hub and half-duplex communication are not used except during debugging.

Logical network systems shall be set up to appropriately design bandwidths that can be used by networks more effectively.

To allow networks to effectively use the bandwidths to which they have access, logical networks should use virtual LAN (VLAN) architectures and develop networks from virtual groups that do not depend on physical connection types.

Under normal conditions, target traffic on subnetworks shall be approximately 25 % when half duplex communication is adopted, and 50 % when full duplex communication is used.

9.7 Wireless network design

9.7.1 General

Wireless networks are vulnerable to radio wave interference from shipboard equipment, its use in controlled networks is not taken into consideration.

When designing shipboard wireless networks, it is necessary to pay full attention to compatibility among various devices in the networks, various factors relating to data transmission (e.g. the amount of information, delay time and routes) and safety.

In the design of shipboard wireless networks, it is necessary to calculate in advance the amount of valid data and network load factors when the network load is at its maximum. It is also necessary to consider the expansion of shipboard networks and growth in data traffic.

To implement means of communication that are allowed in various failure scenarios, such as security incidents, designs shall be drawn in consideration of various system states (e.g. initial, failure and normal states).

In shipboard wireless networks, equipment that meets 16425-Wireless-gateway (see 8.2.4.3 and 8.2.4.4) or 460-Wireless-Gateway requirements shall be installed.

9.7.2 Frequency requirement

Currently, there are two frequency bands commonly used for IP communication: the 2,4 GHz and 5 GHz bands. The appropriate frequency shall be selected depending on the required transmission speed (see 8.3.3), the ambient environment and the connected devices.

9.7.3 Frequency interference

In wireless LAN, overlapping frequency channels can cause radio interference, resulting in poor communication performance. The channels shall be designed so that they do not overlap and cause radio interference.

9.7.4 Load design

In wireless networks, full-dual communication is unavailable, as CSMA/CA is adopted. When multiple nodes are connected at the same time with single 16425-Wireless gateway or 460-Wireless gateway units, they do not allow communication at the same time. Therefore, latency time is generated.

In designing shipboard wireless networks, it is necessary to figure out the protocol and traffic (see 8.3) and wireless LAN specifications (see 8.2.4.3) of nodes to be connected.

The signal strength and speed shall be measured in accordance with the pre-survey (see 9.7.8) and the position of the 16425-Wireless gateway or 460-Wireless gateway. The distance from the position and the speed shall be investigated.

The total number of equipment and traffic connected to the 16425-Wireless gateway or 460-Wireless gateway shall determine where, and how many 16425-Wireless gateways or 460-Wireless gateways are to be fitted.

The pre-survey should be carried out on a ship of similar size to the ship on which the wireless on board is to be built. If no similar vessel is available, the pre-survey should be carried out in a space similar to that in which the installation is planned.

The number of nodes can have a direct impact on interference. The available frequency bands shall be taken into account when deciding on the number of units to be installed.

9.7.5 Installation design

The system documentation shall specify the area to be serviced by the shipboard wireless network and the location of the 16425-Wireless gateway or 460-Wireless gateway.

There should be no more than 30 devices connected to a single 16425-Wireless gateway or 460-Wireless gateway. If the number of connected nodes is greater than 30, the number of devices connected to a single 16425-Wireless gateway or 460-Wireless gateway should be reduced by suppressing the signal strength and thereby reducing the service range.

9.7.6 Wireless network security design

For the wireless network design, see 13.1.5.3.

9.7.7 Power supply and voltage

16425-Wireless-Gateway units can receive power from either shipboard electrical outlets or PoE.

When receiving power from PoE, the requirements of 9.4.2.5 shall be observed.

9.7.8 Pre-survey

When building shipboard wireless networks, it is recommended that the following items are measured in advance, using a shipboard with the same specifications:

a) radio wave strength;

b) communication rates;

c) signal-to-noise ratios (SNRs);

d) throughputs.

The preliminary checks shall be carried out using 16425-Wireless-gateway or 460-Wireless-gateway units that are intended to check for radio interference.

The preliminary tests shall be carried out in all frequency bands available to the 16425-Wireless gateway or 460-Wireless gateway.

The preliminary testing e) to h), shall be carried out in a location similar to the actual environment in which the gateway will be used.

Pre-surveys shall be conducted with the 16425-Wireless gateway or 460-Wireless gateway units that are intended for use. The following requirements apply.

e) Pre-surveys shall be conducted in areas where radio wave strength is −65 dBM or higher.

f) Pre-surveys shall be conducted in areas where SNRs are −20 dBM or higher. Noise sources shall be removed if possible.

g) Pre-surveys shall be conducted in areas where there are sufficient communication rates.

h) Pre-surveys shall be conducted in areas where there are more-than-required throughputs.

The areas that meet all requirements are regarded as cells. It is necessary to install 16425-Wireless-gateway or 460-Wireless-gateway units so that cells do not overlap in service areas.

9.7.9 Security design

Restrictions shall be imposed to allow only authorized crew members to enter areas where 16425-Network devices and 16425-Network equipment are installed for purposes other than welfare networks.

If such restrictions cannot be placed, unused ports shall be physically or logically unavailable.

Passwords for 16425-Network devices shall be changed from default passwords.

9.8 Documentation

9.8.1 Network design document

In network design documents, specifications for designing networks shall be written, including at least, the items described in 9.3.

9.8.2 List of equipment (device inventory)

All equipment required for connection with shipboard networks shall be listed individually. Passive (non-powered) devices of the same model and manufacturer may be grouped into a single item. However, criteria for their usage shall be clarified in design documents.

9.8.3 Schematic diagram

A schematic diagram is a drawing which focuses on physical connections between equipment.

When equipment has more than one LAN interface, the (physical) identifiers of destination interfaces shall be clarified.

All cables, codes and devices in network systems, including connected port number, extender connectors and telecommunication outlets, shall be individually identified in the schematic diagram.

The locations of 16425-Network equipment shall be included in the schematic diagram.

Cable lengths shall be included in the schematic diagram.

If power is supplied using PoE, it shall be included in the schematic diagram showing that it is PoE.

The construction manager of the cable shall be included in the schematic diagram.

In cases of different suppliers of cables, plugs and jacks, the responsibility for confirmation of installation and tests shall be decided between the suppliers in advance.

9.8.4 Logical topology diagram

A logical topology diagram is a drawing that shows data flows between 16425-Network devices and 16425-Network equipment (i.e. VLAN diagrams).

VLANs, to which all ports belong (including trunk ports) shall be clarified.

Logical topology diagrams shall be linked with physical devices and cables.

When single ports have more than one IP address, all of them shall be listed.

9.8.5 List of virtual networks

At least the following items shall be managed in the list of virtual networks.

a) VLAN ID

b) VLAN type (Access/Trunk)

c) Network address (e.g. 192.168.0.0/16)

d) Name

e) Purpose

9.8.6 List of interfaces between (virtual) networks

For security reasons, all the interfaces between (virtual) networks shall be documented.

The list of interfaces shall include ports, protocols and services (PPS) for all communications between (virtual) networks.

9.9 Risk assessment (design phase)

Risk assessments shall be carried out and documented at the request of the user.

Both failure and cyber risks shall be considered in the risk assessments.

IEC 31010 may be applied to determine method of risk assessment.

As an example, the requirements for the use of failure mode, effects and criticality analysis (FMECA) are described in Annex B.

NOTE Other risk assessments include FMECA, FMEA, FMEDA, FTA, DFA and STPA.

The documents shall be reviewed and updated at least in cases where a device inventory is created and changed and a major incident occurs.

Wiretapping may be excluded from failure mode for the closed network (no direct connection to internetworking).

10 16425-Network device and cable installation

10.1 General

Unlike land-based offices, installation of 16425-Network devices shall take external factors into account, chief among them water, vibration, and heat. Given these special circumstances, the methods for installing, protecting and cabling the 16425-Network device shall be defined.

10.2 Installation procedure

10.2.1 16425-Network device

10.2.1.1 Environmental resistance

All 16425-Network devices shall be installed under environments set forth in network design documents. Parameter examples to consider include: surrounding temperature and humidity, condensation, collusive/volatile gas and oil-contained air, and dust quantities. To ensure protection from adverse environments, a protective case may be adopted for each device.

10.2.1.2 Considerations for vibration

To keep devices and connectors from being damaged, and connectors from being disconnected by ship vibrations, either 16425-Network devices shall be installed fully away from vibration sources, or anti-vibration efforts shall be made with the use of anti-vibration rubber and other actions. To keep connectors intact, anti-disconnect devices may be adopted.

10.2.1.3 Considerations for noise

To avoid being adversely affected by outside noise, 16425-Network devices shall be installed at locations specified in network design documents. When needed, devices shall also be firmly ground.

10.2.2 Network cable

10.2.2.1 Mechanical protection

To protect network cables from outside, materials set forth in network design documents shall be used. If there is a risk of cables becoming mechanically damaged when being laid, it is better to use damage-resistant cables.

10.2.2.2 Minimum bending radius

10.2.2.2.1 Metal cable

The minimum bending radius specified for the cable shall not be exceeded.

NOTE If the requirements specifying the minimum bending radius are not complied with, performance can be harmed and the cable can be broken.

10.2.2.2.2 Optical cable

Optical cables shall not exceed the specified minimum bending radius, in order to prevent transmission loss due to bending of the cables.

NOTE The excess of the minimum bending radius can harm performance or cause the cable to break. There are two types of minimum bending radius: the fixed bending radius, which indicates the bending radius after the cabling is installed; and the extension bending radius, which indicates the momentarily tolerable bending radius.

10.2.2.3 Tensile load

10.2.2.3.1 Metal cable

When the cable is pulled or hung, the cable's specified tensile load shall not be exceeded.

Whenever possible, cabling routes shall be secured after other cabling has been installed. Metal network cables should be installed with care (e.g. cables should be installed separately). The metal network cables should not be wrapped with power cables, bent or twisted excessively. If cabling is installed vertically,

supports shall be installed at regular intervals to prevent the cable's own weight from exceeding the rated tensile load.

The network cables for PoE power supply shall not be wrapped with other PoE cables.

10.2.2.3.2 Optical cable

When the cable is pulled or hung, the cable's specified tensile load shall not be exceeded.

Optical cables shall be fitted with tension members to prevent the weight of the cables from being pulled.

Secure cabling routes after other cabling has been installed. The optical cables should not be wrapped with other cables, bent or twisted excessively, e.g. optical cables can be installed separately.

If cabling is installed vertically, install supports at regular intervals to prevent the cable's own weight from exceeding the rated tensile load.

10.2.2.4 Bundling

10.2.2.4.1 Metal cable

When bundling cables in a cable way, excessive load should not be put onto the cables.

10.2.2.4.2 Optical cable

When bundling optical cables in a cable way, excessive load should not be put onto the cables.

10.2.2.5 Cable route

In cases where duplicate circuits (main and backup circuits) are required in shipboard network design, those two cables shall follow different routes which shall be as far apart as practicable.

When electromagnetic interferences from other devices are likely, shielded cables specified in network design documents shall be used, and they shall be installed at appropriate locations. It is also effective to keep distances as described in Table 3.

Optical fibre cables and others shall be installed, while avoiding pressurization from other cables.

As network cables tend to suffer declines in performance due to changes in surrounding temperature, they shall be installed under environments meeting conditions specified in shipboard network design documents.

Table 3 — Separation and segregation from noise sources

Status		Minimum separation		
Power line route/ equipment	Single line (or route)	2 kVA or less	2 to 5 kVA	5 kVA or more
No shield	No shield	127 mm	305 mm	610 mm
No shield	Shielded	64 mm	152 mm	305 mm
Shielded	Shielded		76 mm	152 mm

10.2.2.6 Protective cases

Consideration should be taken to use a marine cable with a tension member constantly when using optical cables. Cables shall satisfy the requirements from classifications.

NOTE Requirements of the relevant flag states can apply.

10.2.3 Cable end termination

10.2.3.1 Connector section

Connectors and cables shall be paired and connected as prescribed in network design documents. It is important to consider the following:

— straight or cross connections (T568A or T568B connections, specified in ANSI/TIA-568.0);

— STP or UTP;

— single or stranded cables;

— cable connectors agree with connectors;

— connectors and jacks meet the suppliers' requirements;

— cable core diameters and connector types meet the suppliers' requirements.

10.2.3.2 Earth method

When LAN cables are laid (one side or both sides), the instructions in 8.4.3 shall be followed. In conducting laying work, it is important to ensure that LAN cable drain wires and others are firmly connected with the metal parts of plugs.

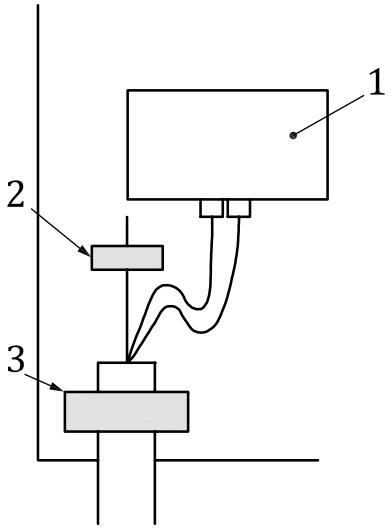
10.2.3.3 Terminal protection

10.2.3.3.1 Terminating metal cables

To prevent the tensile load from being generated on connector devices, metal clamps may be used. To keep connections from bending sharply, connectors with boots may be used. When cable identifications are required in designing networks, boots shall also be adopted.

10.2.3.3.2 Terminating optical cables

As shown in Figure 4, lock optical cables and their tension members in place using metal clamps, to prevent damage from vibration and tension.



Key

1 optical cable HUB
2 metal clamp for tension member
3 cable clamp

Figure 4 — Terminating optical cables

10.3 Installation confirmation

10.3.1 Conductivity confirmation

A conductivity test should be performed to ensure that there are no breaks in the cable.

10.3.2 Wire map confirmation

The test shall be performed to ensure that each pair's connector is in the proper location in accordance with T568A or T568B, as specified in ANSI/TIA-568.0. At this time, the test shall also be performed to check that the appropriate straight/cross connection is in accordance with ANSI/TIA-568.0:2020, 6.2.3.2.

10.3.3 Length confirmation

This test shall be performed to ensure that the cables are not longer than 100 m, and that the cables are not shorter than the originally planned length. If a cable is shorter than the originally planned length, it may be treated as the breakage distance.

NOTE Nearly all cables have better performance than the specification so a distance longer than the actual length is sometimes shown.

10.3.4 Insertion loss test

Insertion loss (dB/100 m) shall be tested. This test shall also be performed to ensure that the insertion loss for each cable is within the rating for that cable in accordance with ISO/IEC 11801-1.

10.3.5 Near end crosstalk loss

Near end crosstalk loss (dB) shall be tested. This test shall also be performed for near end crosstalk loss greater than the rating for each cable in accordance with ISO/IEC 11801-1.

10.3.6 Power meter checking

Measurement of the transmission loss (dB) using a power meter is required. The measured optical loss shall be within the allowable dissipation for the device used (e.g. optical hub or media converter). When measuring the transmission loss, the appropriate calibration wavelength shall be selected for that cable type.

10.3.7 Cable ID

Before installing network cables, a check is required to see whether an item indicating each cable's ID number is attached. After installing the network cables, a check is also required to see whether all characters in the cable's ID numbers can be correctly recognized. These procedures shall be performed regardless of the cable type.

10.3.8 End termination

The termination of the cable shall be carried out in accordance with the manufacturer's equipment instructions.

10.4 16425-Wireless-Gateway installation procedures

10.4.1 Environmental resistance

10.4.1.1 Installation

Electromagnetic immunity and emissions testing of the 16425-Wireless gateway or 460-Wireless gateway shall be conducted in accordance with the installation location. For example, if installed on a ship bridge, the requirements of IEC 60945 shall be met. If installed in an engine control room, the requirements of IEC 60092-504 shall be met.

The 16425-Wireless gateway or 460-Wireless gateway should be installed in an open space and as high as possible.

The environment around of the 16425-Wireless gateway or 460-Wireless gateway shall be free of any interference in the frequency range up to 2 GHz in accordance with IEC 60945, as it cannot be proved that this does not affect the operation of the 2,4 GHz and 5 GHz bands in which the wireless LAN operates. Only products that meet the requirements of electromagnetic field in IEC 60092-504:2016, Table 2 shall be installed.

10.4.1.2 Considerations for vibration

To keep devices and connectors from being damaged and connectors from being disconnected by ship vibrations, either 16425-Network devices shall be installed fully from vibration sources, or anti-vibration efforts shall be made with the use of anti-vibration rubber and other actions. To keep connectors intact, an anti-disconnect device may be adopted.

10.4.1.3 Considerations for noise

To avoid being adversely impacted by outside noise, 16425-Network devices shall be installed at locations specified in network design documents. When needed, devices shall also be firmly installed.

11 Network cable installation and wireless installation test and inspection

11.1 Cable installation

Tests shall be carried out in accordance with Table 4 for 16425-Network device, network cable and optical cable installations, as defined in 10.2 and 10.3. Test and inspection shall be carried out by each construction manager.

The test items listed in Table 4 correspond to the subclauses of Clause 10 in this document.

The results of tests and specifications shall be maintained by the construction manager until completion of the work, after which they shall be retained by the system integrator, for the ship operator and onboard ships. These test specifications shall be applied for transmission frequency of 100 MHz or less.

Table 4 — Installations of the 16425-Network device, network cables and optical cable

Test items	Test methods	Evaluation standards
10.2.1.1 Environmental resistance	Confirm that the 16425-Network device installation requirement in 10.2.1.1 is satisfied.	It should be ensured that the requirements for the installation environments defined in ship classifications or international standards meet the requirements for the installation environments of 16425-Network devices by looking at where they are installed. The installation requirements should be written down in the installation manual.
	Confirm that the 16425-Network devices in the environments are installed as defined under network design specifications.	
10.2.1.2 Considerations for vibration	Confirm that the 16425-Network device installation requirement in 10.2.1.2 are satisfied.	Confirm that there are no vibrations that would add load to 16425-Network devices themselves or their connectors, and write the installation requirements down in the installation manual.
	Confirm that the racks and mounts to which 16425-Network devices are attached do not vibrate.	
	Ensure that there is no extra play so that vibration does not add load to connectors.	
10.2.1.3 Considerations for noise	Confirm that 16425-Network device installation requirements in 10.2.1.3 are satisfied.	Ensure and record that 16425-Network devices have been installed as described in the network design documents so they are not adversely interfered by noise from outside sources.
	Confirm that 16425-Network devices have not been installed near inverters, motors or high-voltage electrical power lines, which can be a source of external noise.	
	Ensure sufficient space is provided, as described in network device installation manuals.	
	Confirm that 16425-Network devices have been installed in accordance with the network device installation manuals.	
10.2.2.1 Mechanical protection	Confirm that the network cable installation requirement in 10.2.2.1 is satisfied.	It is recommended to protect network cables and ensure that they are properly protected as defined in ship classifications or international standards by determining where the cables are being laid. A record should be kept of this.
	Confirm that the network cables shall be protected as defined in network design specifications.	
10.2.2.2.1 Metal cable	Confirm that the network cable installation requirement in 10.2.2.2.1 is satisfied.	Ensure that network cables do not exceed specifications for the minimum bend radius, and write the installation requirements down.
	Confirm that network cables shall not exceed the minimum bend radius in network design specifications.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
10.2.2.2.2 Optical cable	Confirm that the optical cable installation requirement in 10.2.2.2.2 is satisfied	Ensure that optical cables do not exceed the required minimum bend radius, and keep a record of it.
	Confirm that optical cables shall not exceed the minimum bend radius designated in network design specifications.	
10.2.2.3.1 Metal cable	Confirm that network cable installation requirements in 10.2.2.3.1 are satisfied.	Confirm that network cables are not under tensile load or twisted with their own weight, and write this down. Also, ensure that network cables are not lashed together with power cables, and write the installation requirements down.
	When network cables are laid vertically, they shall be lashed down so as not to be under tensile load.	
	Ensure that installation instructions are given for instructions for laying the network cables without kinks.	
	Ensure there are no twists on the network cables where there is no outer skin.	
	If the installation procedure restricts the tying of network cables and power cables together, ensure that the network cables are laid according to the restrictions.	
	Ensure that the part of the network cable without the outer shell is not placed together with the power cable in single groups.	
	Ensure that the PoE network cables are not placed together in single groups.	
10.2.2.3.2 Optical cable	Confirm that the network cable installation requirements in 10.2.2.3.2 are satisfied.	Confirm that optical cables are not under tensile load or twisted with their own weight, and write this down. Also, ensure that network cables are not lashed together with power cables, and write the installation requirements down.
	When optical cables are laid vertically, they shall be lashed down so as not to be under tensile load.	
	Ensure that installation instructions are given for instructions for laying the optical cables without kinks.	
	Ensure there are no twists on the optical cables where there is no outer skin.	
	If the installation procedure restricts the tying of network cables and power cables together, ensure that the network cables are laid according to the restrictions.	
	Ensure that the part of the optical cable without the outer shell is not placed together with the power cable in single groups.	
10.2.2.4.1 Metal cable	Confirm that network cable installation requirements in 10.2.2.4.1 are satisfied.	Using a network tester, confirm that the insertion loss, near-end crosstalk loss (NEXT), power sum near-end crosstalk loss (PSNEXT), equal level far end crosstalk (ELFEXT), power sum equal level far end crosstalk (PSELFEXT) and return loss are within the limits specified in ISO/IEC 11801-1, ensuring that the parts where network cables are placed together are not overloaded, and write the installation requirements down in the installation manual.
	Confirm that the parts where network cables are put together are not overloaded, e.g. ensure that network cables are not placed together in such a way that a heavy load would damage their coating.	
10.2.2.4.2 Optical cable	Confirm that optical cable installation requirements in 10.2.2.4.2 are satisfied.	Using a tester, confirm that optical cables are not overloaded and that it is within the specified range as specified in ISO/IEC 11801-1. Write the installation requirements down in the installation manual.
	Confirm that the parts where optical cables are put together are not overloaded.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
10.2.2.5 Cable route	Confirm that network cable installation requirements in 10.2.2.5 are satisfied.	Ensure that network cables have been laid as specified in network design instructions, and keep a record of it.
	When network cables are duplicated, ensure that they are wired on different routes according to the installation chart.	
	Confirm that network cables to be used are of the shield types described in network design specifications.	
	Confirm that network cables to be used are the twist types described in network design specifications.	
	Confirm that network cables to be used are the category types described in network design specifications.	
10.2.2.6 Protective cases	Confirm that optical cable installation requirements in 10.2.2.6 are satisfied.	Ensure that network and optical cables meet the requirements of ship classifications and keep a record of it. The requirements of the relevant flag state can apply.
	Confirm that optical cables meet the requirements of the classification, with tension members in place at all times. The requirements of the flag state can apply.	
10.2.3.1 Connector section	Confirm that network cable and the connector installation requirement in 10.2.2.6 are satisfied.	Ensure that network cable modular jacks are equipped as described in network design specifications. Write the installation requirements down in the installation manual.
	Confirm that network cables are connected as described in network design specifications (A or B connections).	
	Check whether the specifications of network cables and connectors in use conform with each other.	
	Confirm that connectors and jacks in use meet network design specifications.	
	Confirm that the core wire diameters of network cables and the types of connectors in use meet network design specifications.	
10.2.3.2 Earth method	Confirm that network cable installation requirements in 10.2.3.2 are satisfied.	Check whether the earthing of network cables is done as described in network design specifications. Write the installation requirements down in the installation manual.
	The earthing of shield network cables shall be carried out as described in network design specifications.	
	Check to see whether the drain wires of shield network cables are firmly connected to the metal parts of plugs.	
10.2.3.3.2 Terminating optical cables	Confirm that optical cable installation requirement in 10.2.3.2 are satisfied.	Confirm that optical cables are secured using metal clamps and tension members. Write the installation requirements down in the installation manual.
	Ensure that optical cables are secured using metal clamps and tension members.	
10.3.1 Conductivity confirmation	Confirm that network cable installation requirements in 10.3.1 are satisfied.	Ensure that all core wires (normally four pairs of eight wires) and drain wires (in the case of STP cables) of cables are not broken or short-circuited. Write the installation requirements down in the installation manual.
	Check each cable's wire maps with network testers.	
10.3.2 Wire map confirmation	Confirm that network cable installation requirements in 10.3.2 are satisfied.	Ensure that wire connections are made as designed without having split pairs. Write the installation requirements down in the installation manual.
	Check each cable's wire maps with network testers are capable of detecting split pairs.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
10.3.3 Length confirmation	Confirm that network cable installation requirements in 10.3.3 are satisfied.	Ensure that the longest channel length of each pair is 100 metres or less, and write the installation requirements down.
	Measure channel cable lengths with network testers. When more than one cable is connected to 16425-Network devices via extender connectors and telecommunication outlets (9.4.1.4), measurements shall be made at both ends including all cables connected to equipment (see Figure 3). It is desirable to take measurements while main engines/power generation engines are turned on.	
10.3.4 Insertion loss test	Confirm that network cable installation requirements in 10.3.4 are satisfied.	Ensure that measured insertion losses of channels are the values prescribed in ISO/IEC 11801-1 or less. Keep a record of this.
	Measure channel insertion losses with network testers. When more than one cable is connected to 16425-Network devices via extender connectors and telecommunication outlets (9.4.1.4), measurements shall be made at both ends including all cables connected to equipment (see Figure 3).	
10.3.5 Near end crosstalk (NEXT) loss	Confirm that network cable installation requirements in 10.3.5 are satisfied.	Ensure that measured NEXTs of channels are the threshold values in ISO/IEC 11801-1 or less, and keep a record of it.
	Measure channel NEXTs with network testers. When more than one cable is connected to 16425-Network devices via extender connectors and telecommunication outlets (9.4.1.4), measurements shall be made at both ends including all cables connected to equipment (see Figure 3).	
10.3.6 Power meter checking	Confirm that network cable installation requirements in 10.3.6 are satisfied.	Ensure that measured power losses of channels are the threshold values in ISO/IEC 11801-1 or less. Write the installation requirements down in the installation manual. Calculate threshold values with link lengths, connector amounts, fusion splicing amounts and the power loss of each factor.
	Channel power loss measurements shall be in accordance with ISO/IEC 14763-3.	
10.3.7 Cable ID	Confirm that network cable installation requirements in 10.3.7 are satisfied.	Ensure that cable IDs are visible both before and after cables are laid. Write the installation requirements down in the installation manual.
	Visually inspect cable labels for all the cables before installation. Visually inspect cable labels for all the cables after installation.	
	Confirm that the network cable installation requirements in 10.3.8 are satisfied.	
	Recommended items to be checked with metal cables / Good example / Bad example	

Table 4 *(continued)*

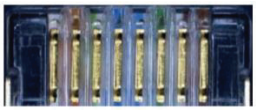
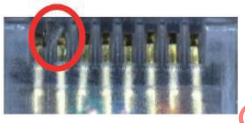
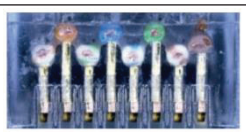
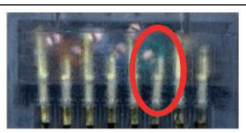
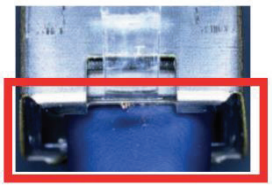
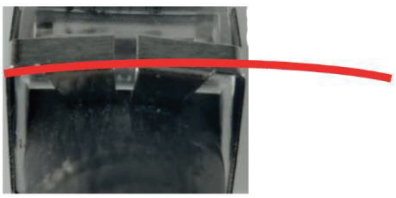
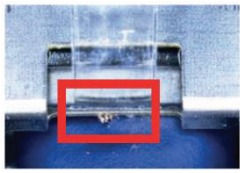
Test items	Test methods			Evaluation standards
10.3.8 End termination	Confirm that there are no abnormalities in each pin, such as rust, taint (e.g., oil and dust), distortions, shaved parts and discoloration.			Ensure that terminal treatments are made in accordance with the manufacturers' standards and write the installation requirements down. Typical examples are shown on the left in the test methods column.
	Confirm that there are no abnormalities in the plastic parts, such as scratches, distortions and discoloration, and the plastic parts are parallel and arranged at equally spaced intervals.			
	Ensure that there are no foreign particles or dust attached to the plugs.			
	Confirm whether cable coatings reach inside the plugs, and whether the length of the unwound parts of the core wires are coated.			
	Ensure that the plug pawls are not broken. Even when the pawls are pushed and flattened, they shall return to their original state.			
	Ensure that the pins are not distorted.			
	Ensure that each core wire reaches the end of the plug.			

Table 4 *(continued)*

Test items	Test methods			Evaluation standards
	When LAN cables are thick, check to see whether the plugs are under load.			
	In case of STP plugs, check to see whether drain cables or cable shields are firmly attached to the metal parts of the plugs.			

11.2 16425-Wireless Gateway installation confirmation

Tests shall be carried out in accordance with Table 5 for 16425-Wireless gateway installations defined in 10.4.

These test standards shall be applied for transmission frequency of 100 MHz or less.

Table 5 — 16425-Wireless gateway installation confirmation

Test items	Test methods	Evaluation standards
10.4.1.1 Installation	Confirm that the installation procedure in 10.4.1.1 for the 16425-Wireless gateway device is satisfied.	It should be ensured that requirements for the installation environments defined in ship classifications or international standards meet the requirements for the installation environments of 16425-Wireless gateway devices by looking at where they are installed. The installation requirements should be written down in the installation manual.
	Confirm that 16425-Wireless gateway devices have been installed in the environments defined in network design specifications.	
	Ensure that the electromagnetic emission requirements only meet the requirements of IEC 60945:2002, 9.2 and 9.3.	
10.4.1.2 Considerations for vibration	Confirm that the 16425-Network device installation requirements in 10.4.1.2 are satisfied.	Ensure that vibration does not add load to 16425-Wireless gateway devices themselves or connectors. Write the installation requirements down.
	Confirm that racks and mounts to which 16425-Wireless gateway devices are attached do not vibrate.	
	Ensure that there is no extra play so that vibration does not add load to connectors.	

Table 5 *(continued)*

Test items	Test methods	Evaluation standards
10.4.1.3 Considerations for noise	Confirm that 16425-Network device installation requirements in 10.4.1.3 are satisfied.	Confirm that 16425-Wireless gateway devices have been installed as described in the network design documents so as they are not adversely influenced by noise from outside sources.
	Confirm that 16425-Network devices shall not be installed near inverters, motors or high-voltage electrical power lines, which can be a source of external noise.	
	Ensure to provide sufficient space as described in 16425-Wireless gateway device installation manuals.	
	Confirm that 16425-Network devices are installed in accordance with the installation manuals for the 16425-Wireless gateway device.	

12 Network operation

12.1 General

Ship managers shall continue to operate shipboard networks in accordance with operation plans. Ship managers shall also compile maintenance reports regularly and when trouble arises, record operations and store them for the time designated in operation plans. When there are changes, additions or deletions in network topologies, definition information, software versions or installed devices, ship managers shall formulate maintenance reports, and store them for the time designated in operation plans.

12.2 Identify vulnerabilities

12.2.1 Operation policy and procedure

Operators shall put basic shipboard network operation policies and procedures in writing. Such policies and procedures shall be referred to when changes are made in the future in new network configurations, to confirm the intentions of the original operation policies and procedures are maintained and not compromised.

12.2.2 Inventory and assessment

12.2.2.1 Network inventory list

Operators shall produce inventory lists of devices and cables that constitute shipboard networks with support from shipyards and suppliers before ships are delivered. While ships are in service, such documents shall be maintained, revised and managed on shipboard and on shore.

12.2.2.2 Network Topology

Network topologies are the physical and logical diagrams of shipboard networks. Operators shall formulate network topologies with support from shipyards and suppliers before ships are delivered. Such network topology documents shall be appropriately maintained and managed throughout the ships' life cycles, and stored on shipboard and on shore.

The inventory list of equipment hardware and software shall include, at a minimum, the 16425-Network equipment and 16425-Network device details specified in ISO 24060: 2021, 4.1.2.

12.2.2.3 Network Risk Assessment

Operators shall assess shipboard network risks, put the outcome in writing and compile risk assessment reports.

12.3 Develop protection and detection measures

12.3.1 Policy and procedure

To ensure that shipboard networks continue to be operated in accordance with operation plans, operators shall prepare policies and procedures for preventing abnormalities. Operators shall also appropriately monitor operations and take actions to detect troubles immediately when they occur.

Policies and procedures to prevent abnormalities should comply with functional safety standards (e.g. the IEC 61508 series).

12.3.2 Access control

12.3.2.1 Physical access

As for the comings and goings of individuals who can physically access shipboard networks, visitors from outside who are not crew members are permitted to access networks for admitted purposes only, if they present proper identification and other documents. Physically recorded data on security devices shall be safely maintained and managed.

Ship owners shall define security boundaries to protect areas covering IT and OT networks. The locations and strengths of boundaries shall be decided based on risk assessment results.

For protection from physical threats, see 13.1.4.2.

12.3.2.2 Shipboard network access

Policies and procedures for accessing shipboard networks shall be formulated. It is necessary to decide who can access the networks, when the networks can be accessed and what can be accessed through shipboard communication and network paths. Operators shall devise policies and procedures for communication to shipboard IT and OT networks and control over interfaces, and put them in writing with support from shipyards and suppliers. Policies shall be implemented while ensuring consistency with the security and privacy requirements of entire operating companies and/or organizations. Overland managers, ship masters and other crew members shall tightly cooperate with each other to formulate and implement procedures.

For protection from logical threats, see 13.1.4.1.

12.4 Response and recovery

12.4.1 Contingency plan

Contingency plans shall contain a series of previously defined instructions and procedures to take appropriate measures when detecting shipboard network faults in a timely fashion, ensure that ships continue to operate and minimize impact on the natural environment.

12.4.2 Response to shipboard network incidents

Measures shall be mulled and implemented to take appropriate actions when shipboard network faults are detected. Operators shall ensure shipyards and suppliers take appropriate action. Shipyards and suppliers shall provide documents on measures and procedures to address shipboard network faults before ships are delivered.

Documentation on measures and procedures for dealing with shipboard network failures should comply with functional safety standards (e.g. the IEC 61508 series).

12.4.3 Recovery from shipboard network incidents

Measures shall be mulled and implemented to rebuild network functions and services in which troubles occurred due to shipboard network failures. Operators shall ensure shipyards and suppliers take appropriate

measures. Shipyards and suppliers shall provide documents on recovery procedures for networks and systems before ships are delivered.

12.5 Maintenance

12.5.1 Maintenance policy and procedure

Operators shall define policies and procedures for managing changes so that they can appropriately record revisions in documents and drawings as well as relevant histories when there are changes in various documents on network operations (mainly those on the subjects set forth in 12.2 to 12.5) while networks are in operation.

12.5.2 Maintenance document and report

When there are changes in various documents on network operations (mainly those on the subjects set forth in 12.2 to 12.5) while networks are in operation, operators shall appropriately revise the documents and drawings, and compile maintenance reports on relevant histories in accordance with the policies and procedures in 12.2.

When needed, operators shall build mechanisms to compile maintenance reports to be able to confirm the versions of software programs working in 16425-Network devices and the 16425-Network equipment.

Operators shall also confirm that interfaces and functions work as expected when maintenance work is completed, and record results in maintenance reports.

13 Network cyber security

13.1 Network cyber security requirements

13.1.1 General

For controlled networks in 16425-Networks and 460-Networks connecting shipboard equipment and controlled networks connecting IT equipment, protection is necessary from internal threats and threats from outside of the networks to which they are linked. This clause describes ways to protect such networks from direct threats from inside of ships and threats from inside shipboard networks.

Devices that make up networks (see Clause 8) shall be installed in places designated as “restricted areas” where security level 1 or higher is applied [see IMO ISPS Code Part B (2020)].[32] If they cannot be installed in such designated areas, protection shall be made from physical threats in accordance with 13.1.6.2.

13.1.2 Cyber security management system

13.1.2.1 General

In executing cybersecurity management and making risk assessments, it is important to consider the Guidelines on Security Onboard Ships.[27]

By building and operating cybersecurity management, the understanding of risk management can be promoted among shipboard users, ship owners and ship management companies. Highly conscious cybersecurity efforts can also be expected. By conducting cybersecurity management, the risk of cyberattacks can also be reduced.

When managing cybersecurity, it is necessary to clarify basic policies and action standards for security. Therefore, in addition to the crew members in charge of ship operations, the ship owners and managers shall also be responsible for cybersecurity management.

If requirements for cybersecurity of products and systems are already specified, existing standards can take precedence.

13.1.2.2 Policy

Basic policies stipulate philosophies and guidelines for entire organizations, represent a whole picture of security management and act as guidelines and policies for the security of an entire organization.

NOTE For example, basic policies show why cybersecurity management is necessary and what policies are adopted to safely operate ships.

When developing policies, the following points shall be considered.

a) Clarify assets to be protected;

b) Clarify people to whom policies apply;

c) Describe policies as specifically as possible;

d) Make policies feasible;

e) Consider how policies are implemented and maintained;

f) Clarify penalties to impose on violations to keep policies from becoming dead letters.

13.1.2.3 Safeguard

In safeguard, specific protective measures and standards are incorporated for each equipment and network. In this document, protective measures are set forth for such equipment and networks.

13.1.3 Operation plan design

13.1.3.1 Security scenarios

13.1.3.1.1 General

The 16425-Network equipment and 16425-Network devices connected with shipboard networks are vulnerable to threats from shipboard equipment in the networks. From outside, they are vulnerable to threats from uncontrolled networks, such as shipboard and outboard devices. As such, shipboard networks shall be protected from not only internal threats but also external threats.

13.1.3.1.2 Internal threats scenarios

As for threats from inside of shipboard networks, the following scenarios can be envisaged:

a) PCs infected with malware can infect other equipment in networks with the malware.

b) Equipment can be infected with malware when REDS is attached.

c) Users can intentionally delete files or data from shipboard equipment.

d) Users can accidentally delete (lose) files or data from shipboard equipment.

e) Equipment can be physically destroyed.

f) Unauthorized access can be made to keep equipment from operating as usual.

g) Falsification data can be produced to keep equipment from operating as usual.

h) Network services can be discontinued or brought down by many broadcasts as well as ICMP or IGMP packets (networks and systems can go down in DoS attacks).

Shipboard equipment to be connected with shipboard networks shall meet the requirements set forth in 8.2.4 to eliminate threats from inside of networks to other nodes.

13.1.3.1.3 External threats scenarios

As for threats from outside of shipboard networks, the following scenarios can be envisaged.

a) Threats can be made from unprotected wireless networks.

b) Malware from other shipboard networks can infect 16425-Network equipment.

c) Having remotely logged into 16425-Network equipment, shipboard network users can delete files or data or change settings.

d) Having been installed on shipboard equipment as attack agents, back doors can directly damage the equipment through switches, routers and other network infrastructure facilities.

e) Data can be leaked or falsified with the following attacks that can be made through other shipboard networks whose backbones are not appropriately controlled:

   1) SQL injection attacks;

   2) OS command injection attacks;

   3) LDAP injection attacks;

   4) DoS/DDoS attacks;

   5) buffer overflow attacks;

   6) session highjack attacks;

   7) port scan attacks;

   8) SYN flood attacks.

For security requirements for protection against threats from outside of shipboard networks to 16425-Networks, see 8.2.4.

13.1.4 16425-Network equipment access security

13.1.4.1 General

16425-Network equipment shall provide user authentication functions for changing device configurations. Authentication examples include passwords and key cards.

In case of authentication with passwords, the following requirements shall be met. Some manufacturers require long and/or complex passwords, ban certain words and limit additional passwords.

13.1.4.2 User authorization

To control the access to devices (e.g. changing device configurations), user authentication functions shall be provided. Authentication examples include passwords and key cards.

If the equipment has the functionality for software maintenance by crew or service personnel, the equipment shall have a mechanism to identify and authorize users to restrict the operation and use of resources. Appropriate authorization shall be assigned to the user. Only operations and use of resources consistent with the authorization shall be permitted.

The device shall have at least two authorisations to restrict its operation: general user and administrator with maintenance mode. The identification of the user is carried out by means of an identification and password, called an account, or by means of a physical key authorization. In the case of multi-factor authentication, a combination of these is used. It shall be possible to restrict the operation of the system by using tools that are restricted to service personnel.

In case of authentication with passwords, the following characteristics shall be applied:

— long and/or complex passwords;

— certain words are banned;

— additional passwords are limited.

13.1.4.3 Remote access control

The equipment shall ensure the integrity of transmitted information.

The equipment shall employ cryptographic mechanisms to recognize changes to information during communication.

13.1.4.4 Remote session

The equipment shall have the capability to terminate a remote session either automatically after a configurable time of inactivity or manually by the user who initiated the session.

13.1.4.5 Communication integrity

The system shall protect the integrity of transmitted information.

The system shall employ cryptographic mechanisms to recognize changes to information during communication.

13.1.4.6 Authorization feedback

The equipment shall obscure feedback during the authentication process.

13.1.5 Wireless network access authentication method

13.1.5.1 General

To ensure the security of the wireless LAN, both WPA3 personal and WPA2 personal authentication methods shall be available.

The MAC address authentication function may be used.

13.1.5.2 Wireless network access encryption

The encryption shall be able to use AES.

13.1.5.3 Use control for portable and mobile devices

Portable PCs and mobile devices to be linked with the 16425-Wireless-Gateway shall be protected from the risks of malware infections and information leakage. When the wireless network system supports the use of portable and mobile devices, the following shall apply:

a) limit the use of portable and mobile devices as required by design;

b) restrict code and data transfer to/from portable and mobile devices.

NOTE Port limits / blockers (and silicone) can be accepted for a specific system.

13.1.6 Network design

13.1.6.1 Protection from logical threats

13.1.6.1.1 General

System defences consist of malware infection prevention, host-based firewalls, host-based intrusion prevention and user notifications. They are related to environments in which equipment is installed. Measures to prevent malware infections can be taken depending on the equipment used or the environments in which equipment is installed. Examples of environments in which system defences are provided are equipment installed in networks compliant with IEC 61162-460 and this document.

NOTE Ship owners are responsible for natural disasters and restoration plans, which are deemed to be included in integrated safety management plans (ISMPs) for ships.

13.1.6.1.2 Malware protection requirements

System defences for malware protection are provided with one or several of the following items.

a) Devices to be installed on networks compliant with IEC 61162-460 or this document, and devices compliant with ISO 19847 designed to be installed on networks compliant with this document.

b) Devices designed to be installed on controlled networks that are not compliant with IEC-61162-460 or this document. For this security alternative, security measures specified in IEC 61162-460 or this document shall be taken. Examples are measures approved by IEEE 802.1X-, RADIUS and DIAMETER;

c) Devices that do not have accessible interfaces that can be penetrated by malware.

Examples of such devices are embedded systems that do not have operating systems but do have physical interfaces that can be penetrated by malware. More specific examples are the serial line specified in IEC 61162-1, the IMO radio (frequency) interface offshore wireless communication or specific functions of navigation systems (in other words, radio interfaces that cannot transfer files).

d) Devices that do have accessible interfaces that can be penetrated by malware.

NOTE 1 “Accessible interfaces” refer to interfaces that can be accessed without tools or keys. Examples include USB ports, which are used to read data files; serial programming or debug ports; and network ports.

NOTE 2 This alternative method is typical in on-the-shelf computers with no special configurations.

Such equipment shall not be directly connected to networks compliant with IEC 61162-460 or this document compliant network. They shall be connected to controlled 460-Gateway or 16425-Gateway networks stipulated in IEC 61142-460.

Furthermore, the following procedures are also necessary.

If equipment contains malware protection software modules, there is a possibility that malware protection pattern files are updated. As for equipment with anti-malware software, applications shall meet the performance requirements established by manufacturers, on the condition that protective software against malware and pattern files are constantly updated.

Manufacturers shall obtain documented procedure approval from type approval authorities. To this end, it is necessary to describe in detail methods to assess and record the effect on equipment of updating anti-malware definition files or software. This procedure guarantees that specific types of updating do not have negative impacts on the compliance of intended functions or equipment.

NOTE 3 This updating procedure is equal to the documented quality procedure for assessing the equipment’s chart updating (data files) and chart engine updating (software).

Installation and operation manuals shall contain explanations on ways to update anti-malware measures as necessary. Such manuals shall at least describe the conditions on which updates shall be made. When the

maximum amount of time passes since the last updates of the malware prevention modules, users shall be advised that they are out-of-date, and notified not to use these old modules.

13.1.6.1.3 Denial of service requirements

Denial of service (DoS) attacks are a broad range of cyberattacks aimed at blocking the use of systems connected to networks, jeopardizing security and causing eventual damage. When DoS attacks are succeeded through network connections, they are used as springboards to silence target devices that attackers can impersonate to have further access or control. Made either directly or indirectly, attacks cause errors and increase network traffic until victims cannot execute the functions that are intended. They eventually lead to allowing attackers to fulfil their goals or giving them more opportunities to abuse.

DoS attacks use network protocols that are normally useful and standard network services, communicate with nodes in networks and rapidly increase traffic to damage victims while hiding attack sources. Attacks can cause traffic floods, and if this is the case, it is necessary to refrain from establishing normal transaction channels but to use low bands that are not recorded in logs.

In a broader sense, DoS attacks include direct physical actions to disable devices and indirect actions to do so, by damaging essential parts of electrical power sources, heat management devices and other functions.

System defences against DoS attacks are made with one or a combination of the following items.

a) Devices which are compliant with IEC 61162-460 or this document, designed to be installed in networks which are compliant with IEC 61162-460 or this document. This option, based on IEC 61162-460, includes a function to monitor networks (including a function to monitor planned load balancing) and rules for firewalls, routers, switches and gateways.

b) Inside interfaces of closed networks that are not connected to outside or do not have equivalents. There are no requirements for devices inside networks that are physically protected and not connected to outside, such as steering gear control system devices.

c) Other devices

   System level:

   Manufacturers shall establish appropriate boundaries and network actions that are useful in reducing DoS attacks. In device installation manuals, it is necessary to take in context boundary lines and network actions to eliminate DoS attacks. Examples are as follows.

   1) Firewalls as well as firewall, router and switch filtering.

   2) Redundant network connections.

   3) Load balancing.

   4) Bandwidth control (service quality).

   5) Physical separation of network components.

13.1.6.1.4 Network segmentation

Networks of different systems shall be physically and/or logically segmented. Networks of control systems, non-control systems, critical control systems and non-critical control systems shall be segmented from each other.

13.1.6.2 Protection from physical threats

13.1.6.2.1 General

The shipboard data server shall be protected from physical damage, such as theft, natural breakage and intentional destruction. The shipboard data server should be installed in the restricted areas designated

in the IMO ISPS Code Part B, 2020, 9.18 and 9.21.[32] When the shipboard data servers cannot be installed in these designated restricted areas, protection shall be provided from physical threats, as instructed in 13.1.6.2.2 to 13.1.6.2.5.

13.1.6.2.2 Installation requirements

As for places to install the shipboard data server, the ship owner shall create policies and develop procedures to control access in accordance with risk assessments. To prevent unauthorised access, the shipboard data server shall be installed in locked rooms, on locked racks, in locked cabinets or in locked consoles. Keys shall be appropriately managed so that only the ship manager has access.

13.1.6.2.3 Connection cables

Communication cables to be connected with the shipboard data server shall not be casually laid on the floor to keep away from damage and disconnection.

13.1.6.2.4 Power source management

Electric-power supply cables to be connected with the shipboard data server shall be protected from damage and disconnection.

13.1.6.2.5 Interfaces for removal devices

13.1.6.2.5.1 General

The number of points with which removable devices are connected shall be limited to the minimum necessary for operation and maintenance.

13.1.6.2.5.2 Unused connection points

Unused connection points shall be protected from easy access with one of the following options:

a) blocks by tools or keys;

b) logical invalidation (which cannot be validated);

c) invalidation with settings requiring authentication.

13.1.6.2.5.3 Operation protection

Connection points used for access to data storage shall be configured to permit connection only to data source identified as USB device class 08h (USB mass storage).

Other connection points (other USB device classes and non-USB devices) shall be blocked from easy access to avoid connection and use of a different device than intended, e.g. by means of a tool or key or by password-protection (disable/enable) in the device set-up.

The manufacturer shall provide information about the technology used and how the connection point fulfils the requirement to limit connection to its intended operation.

13.1.6.2.5.4 Executable program file verification

The shipboard data server shall have prohibited all automatic execution from REDS, including auto-run from USB and CD/DVD. Manual execution of any type of file from REDS shall only be possible after passing authentication for accessing the executable content of the REDS. Manual execution shall be possible only for the files that are verified before execution, using digital signature or special keys.

NOTE 1 A digital signature method is based on a private/public key pair. Typically, a hash-function is used, for example the SHA-2 family. Use of MD5 and SHA-1 is now discouraged (see ISO/IEC 10118-3).

NOTE 2 Special keys can be values calculated from the delivered data using a specified function and compared against a known and expected value, both the function and the value being specified by the trusted source or sender.

13.1.6.2.5.5 Non-executable data verification

All unfeasible data in REDS shall be verified using digital signature or a special key before used on the equipment.

13.1.6.2.6 Protection (others)

The shipboard data server shall protect interfaces that are not used for operations.

13.1.6.2.7 Equipment maintenance

To ensure the continuous availability of the shipboard data server, the manufacturer shall write down maintenance methods in maintenance manuals for appropriate maintenance.

13.1.6.3 Wireless network security design

13.1.6.3.1 Authentication protocol

To ensure security for wireless LANs, either the WPA3 personal or WPA2 personal authentication protocol shall be used.

NOTE When MAC addresses are approved, the risk of unauthorized access from outside can be remarkably reduced.

13.1.6.3.2 Encryption

For encryption, the AES shall be used.

13.1.6.3.3 Login password

Administrator passwords for accessing 16425-Wireless gateway units shall be made of up of 10 or more letters and a combination of three of the following four sets: numeric characters, uppercase and lowercase alphabet letters and special characters.

Passwords for general users shall consist of eight or more letters, which shall include two of the following sets: numeric characters, uppercase and lowercase alphabet letters and special characters.

Passwords shall not be identical to usernames or words listed in the dictionary but shall be random, meaningless words.

Passwords shall be kept confidentially to prevent others from gaining access to them.

13.1.6.3.4 ESSID

ESSIDs shall be stealthy and not be accessed easily.

To keep third parties from making unauthorized access, connections from those not designating EESIDs shall be denied.

Many ESSIDs shall not be defined for single 16425-Wireless-Gateway or 460-Wireless-Gateway units.

NOTE In proportion to the number of ESSIDs defined, BEACON traffic increased for 16425-Wireless-Gateway or 460-Wireless-Gateway units.

13.1.6.3.5 Access key

Access keys shall be made up of 10 or more letters and a combination of three of the following four sets: numeric characters, uppercase and lowercase alphabet letters and special characters.

Access keys shall not be identical to ESSIDs or words listed in the dictionary but shall be random, meaningless words.

Access keys shall be kept confidentially to prevent others from gaining access to them.

13.1.6.4 Risk analysis (cyber)

Risk analyses are not completed after only one execution. When threats occur or the documents described in 9.8 are updated, analyses shall be conducted again.

Annex A
(informative)

Implementing the content provided in this document

A.1 Introduction

When configuring shipboard equipment and systems in accordance with this document to improve communication for shipboard equipment and systems, a number of shipboard equipment with various information platforms may be installed. Thus, it is important to give due consideration to the design of hardware, firmware and software to interconnect separate systems, as well as to the configuration of the systems. This is especially the case where shipboard equipment with various shipboard network are installed. For example, in a single ship, some of the shipboard equipment has information platforms equivalent to computers, while others, including embedded equipment such as control equipment, do not have such shipboard networks.

In general, it is technically challenging to interconnect such equipment in accordance with the specifications of information network systems for shipboard equipment.

This annex is intended to provide detailed examples of technical information that serves as specifications for areas where difficulty is expected.

In this annex, detailed examples of the necessary information for the design of communication network systems for shipboard equipment are described for each grade.

A trial design of the information network system is provided herein for the system architecture, data design and administration, installation and testing of the network.

A.2 Network system design

A.2.1 General

When networks are designed, the processes described in Figure 2 should be followed. Examples of each process are shown in A.2.2 to A.2.5.

A.2.2 Process 1 — organized necessary function

A.2.2.1 General

The shipowner should define the purpose of building the shipboard network, the services to be used (e.g. applications and systems), the parties involved, the target availability, the data required, the means of providing data (e.g. equipment and applications), the location of equipment and applications providing data, possible risks, expansion plans, security management systems and policies and operational plans to achieve this purpose.

A.2.2.2 Terms of use

In terms of use (see 6.2), an overview is given, and requirements are clarified for every service that uses a shipboard network. An example of a format for a service overview and requirements is shown in Table A.1.

Table A.1 — Terms of use

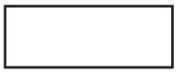
Fields	Description	Max. number
Service ID	IDs for identifying shipboard systems are unique in shipbuilding orders.	1
Service name	Name of shipboard system.	1
Service provider	Name of manufacturers.	1
Service overview	Overview of the services provided by services.	1
Propose of introduction	Purposes of introducing systems.	1
Service users	Roles that receive services onboard and outside ships. When there are more than one, list them all.	unlimited
Service location (ship/ shore)	Locations where services are received.	unlimited
Service level agreement	Targeted occupancy rates.	1
System overview	System configurations and relevant equipment configurations are briefly described. An example is shown in A.2.2.3.	1

A.2.2.3 Example of system overview

An example is shown of system configurations and relevant equipment configurations.

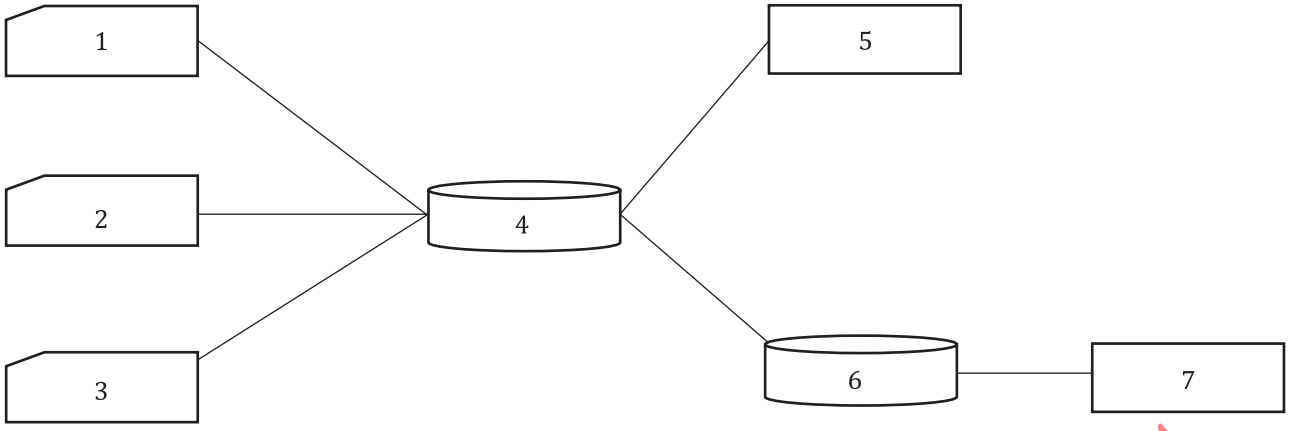
Shipboard equipment that provides data are described in  .

Shipboard equipment that temporarily saves data and relays data to ISO 19847 and ISO 19848 data servers are described in  .

Shipboard equipment that receives data are described in  .

Each equipment has a unique ID on board in each subsystem, and related shipboard equipment is linked with straight lines. An example of a system overview is shown in Figure A.1.

Figure A.1 shows shipboard equipment.



Key

1 AMS
2 VDR
3 ballast system
4 shipboard data server
5 offshore PC
6 mail server
7 on shore PC

Figure A.1 — Example of system overview

System integrators shall interpret data needed by systems that provide services. An example of a format to interpret necessary data is shown in Table A.2.

Requirement function lists are continuously updated until ships are completed, and system integrators manage the lists. Even after completion, they are still updated whenever there are system changes, and ships and ship owners keep a history management record.

Table A.2 — Requirement function list

Fields	Description	Max. number
Service ID	IDs for identifying shipboard systems described in terms of use. Single service IDs can sometimes have more than one system detail.	1
Service name	Names of shipboard systems.	1
System information		
System category	An appropriate system category is selected from among category I, II or III of IACS UR E22 or Navigation or others, and described.	1
Location	Locations of equipment (e.g. H/W, ECR, ER, CCR and the ship's office).	1
Environment requirements	Environment requirements that are met (e.g. IACS UR E10, IEC 60945).	
Security requirements	Security requirements that are met (e.g. ISO 16425, IEC 61162-460, IEC 63154, none, etc.).	1
Manufacture	Manufacturers that provide equipment.	1
Serial No.	Serial numbers with which equipment is uniquely identified.	1
Request Data		
No.	Serial numbers for request data. When more than one data is requested from a single equipment, all information is described.	1
System category	An appropriate system category is selected from among category I, II or III of IACS UR E22 or Navigation or others; and described.	1
TAG ID	Describe the required sentence specified in IEC 61162-1 and the known TAG ID of the measuring point of the machinery system.	1

Table A.2 *(continued)*

Fields	Description	Max. number
Description	Names of necessary data.	1
Type (Sensor/Event)	Types of data (sensor/event) are described.	1
Sampling Rate	Minimum required sampling rates. When only specific sampling rates can be applied, describe it (e.g. 1 ≤ 10, = 5, ≤ 60, etc.).	1

A.2.3 Process 2 — operation plan design

A.2.3.1 General

As for operation plans, information to be managed are organized in accordance with security policies.

While ships are under construction, system integrators manage each item of information and provide it to ship owners. After ships are completed, history management is kept on board the ships and by their owners.

A.2.3.2 Items to manage network devices and cables to be installed

Network devices and cables to be installed are managed. Data for managing 16425-Network devices and cables to be installed are prepared in network designing phases.

A.2.3.3 Details of maintenance

System integrators and owners figure out manufacturers' maintenance organization in preparation for shipboard system maintenance. For information on maintenance organization, whether updated modules are applied or not, how maintenance is given (onsite or remote and periodic or occasional) and the approval of upgrading work and configuration changes, it is necessary to have execution processes and access to control paths.

An example of a format for detailing maintenance is described in Table A.3.

Table A.3 — Details of maintenance

Fields	Description	Max. number
Service ID	IDs for identifying shipboard systems described in terms of use; single service IDs may sometimes have more than one system detail.	1
Maintenance policy		
Module update	Whether there are update modules or not.	unlimited
Maintenance function	How maintenance is provided (e.g. on-site, remote, periodic, occasional).	unlimited
Access control	Access control policies are described (e.g. read, write and execution rights).	unlimited
Maintenance procedure	How maintenance is provided is described.	unlimited

A.2.3.4 Back-ups and log management

System integrators and owners figure out how data are backed up and storages are replaced, where backup media are located, how logs are obtained, log rotations and how logs and data are compressed, saved and monitored. An example of a format for back-ups and maintenance is described in Table A.4.

Table A.4 — Backups and maintenance

Fields	Description	Max. number
Service ID	IDs for identifying shipboard systems described in Terms of use; single service IDs can sometimes have more than one system detail.	1
Backups and maintenance		
No.	Serial numbers are described when a single equipment has more than one backup or logging function.	unlimited
Backup/Log	Types of backups or logging treatments are described.	unlimited
Auto/Manual	It is described whether backups or logging executions are made automatically or manually.	unlimited
Cycle	Intervals of backup and logging executions. Cycles are described as "irregular" when they are not cyclic.	unlimited
Log rotation	Rotation intervals are described when logs that regularly save backups or logs are rotated.	unlimited
Save location	Where backups or logs and rotated logs are saved.	unlimited
Compress	Compression forms are described when backups or rotated logs are compressed.	unlimited

A.2.3.5 Operation of reports

For operation reports, see ISO 21745.

Regulations for trouble are applied to ships and either ship owners or ship managing companies. Trouble reports are submitted to the ship and either ship owners or managing companies. Report formats and periods of time in which to save them are determined in advance. Trouble states (open or close) and approval histories are managed.

A.2.4 Process 3 — installation devices

A.2.4.1 Network equipment management information

Systems to be connected to shipboard networks and network equipment to be connected to systems are managed in accordance with the installation device information. An example of a format for install device information is described in Table A.5.

Table A.5 — Install equipment information

Fields	Description	Max. number
Install device detail		
Service ID	IDs for identifying shipboard systems described in terms of use; single service IDs can sometimes have more than one system detail.	1
Service Name	Names of shipboard systems.	1
Equipment ID	IDs for identifying install devices.	1
System division	Categories of systems (e.g. equipment that provides data: data providers; equipment that saves and distributes data: brokers; and equipment that process and display data after receiving them: subscribers).	1
Date	Dates on which install device information is updated.	1
Version	Versions of install device information.	1
General		
Location	Locations where equipment is installed (e.g. ECR and electric rooms).	1
Environment requirements	Environmental requirements that equipment authorizes or complies with (e.g. IACS UR E10 and IEC 60945).	1

Table A.5 *(continued)*

Fields	Description	Max. number
Security requirements	Security requirements that equipment authorizes or complies with (e.g. this document and IEC 63154).	1
Manufacturer	Manufacturers of equipment.	1
Mode/Reference	Description of whether redundancy configurations can be applied.	1
Occupancy Rate	Occupancy rates of equipment.	1
System Category	An appropriate system category is selected from among Category I, II or III of IACS or Navigation or others and described.	1
System information		
OS/Firmware	Names of the operating system (OS) of the equipment or firmware (if there is no OS).	1
Version	Versions of OS or firmware.	1
Last update	Dates on which OS or firmware are updated.	1
Database System		
No.	Serial numbers of database systems. Information on all database systems is described when a single equipment has more than one different database system.	unlimited
Database name	Names of database systems.	unlimited
Version	Versions of database systems.	unlimited
Supplier	Suppliers of database systems.	unlimited
Account information		
No.	Serial numbers of accounts. Information on all accounts is described when a single equipment has more than one account.	unlimited
OS/Software	Of OSs and software, which system's account information is described.	unlimited
User/roll name	Whether accounts with information on individual users or on roll numbers are described.	unlimited
ID	Information for identifying users or roll accounts.	unlimited
Authority	Approval methods of and information on users or roll accounts (e.g. passwords).	unlimited
Communication Interface		
No.	Serial numbers of communication interfaces. Information on all is described when a single equipment has more than one interface.	unlimited
Physical Layer	Media on the physical layers of communication interfaces are described (e.g. category cables, optical cables, wirelesses, etc.).	unlimited
Address	Addresses of communication interfaces (e.g. IP addresses and UIDs).	unlimited
Port No.	Port no.	unlimited
Link speed	Available link speeds. When "automatic negotiation" is accommodated, describe so [e.g. 10 Mbps, 100 Mbps and 1,000 Mbps (auto)].	unlimited
Cable requirement	Standards for cables to be used (e.g. Category 5E and Category 6A).	unlimited
Shield	Whether shields are needed is described.	unlimited
Cable earth	Whether earthing is needed and how they are applied (single or both sides) are described.	unlimited
Frequency	Bandwidth that equipment follows (e.g. 2,4 GHz and 5 GHz).	unlimited
Encryption	Encryption schemes that equipment follows.	unlimited
IEEE standard	IEEE standards that equipment follows (e.g. IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n and IEEE 802.11ac).	unlimited
Output Information		

Table A.5 *(continued)*

Fields	Description	Max. number
No.	Numbers of sessions when data are output are described. All sessions are described when data are output from a single equipment to more than one unit of equipment or system.	unlimited
Output port no.	Number of ports to which data are output. Physical communication port numbers are described.	unlimited
Protocol	Types of protocols (e.g. ISO 19847, IEC 61162-450, https, etc.).	unlimited
Physical layer	Media on the physical layers of communication interfaces (e.g. categories, cables, optical cables, wirelesses).	unlimited
Cable category	Category types of cables (e.g. 5E and 6A)	unlimited
Source port	Destination port numbers of IP communications. They can be omitted when variable.	unlimited
Destination port	Destination port number of IP communications.	unlimited
Format	Communication formats (e.g. ISO 19848, IEC 61162-450 and csv).	unlimited
Sampling Rate	Transmission intervals.	unlimited
TCP/UDP	Either TCP or UDP is described.	unlimited
Unicast/Multicast	Either Unicast or Multicast is described.	unlimited
Occupancy Rate	Occupancy rates are described.	unlimited
Ave. Traffic	Average communication traffic (kB/s).	unlimited
Max. Traffic	Maximum communication traffic (kB/s).	unlimited
Timing	Timing is described at which maximum communication traffic is recorded.	unlimited
Redundant	Output port numbers for redundancies are described when there are redundancies.	unlimited
Remark	Supplemental information on output information is described.	unlimited
Fields Information		
Output No.	The session port in output information from which data are output is described.	unlimited
No.	Serial numbers of output date items. In output numbers, they are unique.	unlimited
Description	Names of output date items.	unlimited
TAG	Tag IDs of output data items.	unlimited
Analogue/Event/Alert	Types of output data items.	unlimited
Remark	Supplementary information on output data items is described.	unlimited
Input Information		
No.	Numbers of sessions in which data are received. All are described when a single equipment receives data from more than one unit of equipment or system.	unlimited
Send Data Provider equipment ID	Equipment IDs of data providers that receive data are described.	unlimited
Output no.	Numbers output data from shipboard equipment are described.	unlimited
Input port no.	Physical port numbers that shipboard equipment receive are described.	unlimited
Ave. traffic	Average traffic of relevant output numbers described by shipboard equipment (kB/s).	unlimited
Max. traffic	Maximum traffic of relevant output numbers described by shipboard equipment (kB/s).	unlimited
Traffic sum.	Average traffic calculated by input port numbers of input information is described.	unlimited
Max. Traffic sum.	Maximum traffic calculated by input port numbers of input information is described.	unlimited

A.2.5 Process 4 — Network design

Tables A.1, A.2 and A.5 show information on networks that meet the requirements in Clause 9. The network design document contains information that can identify the validity of each design for the network device, network equipment, code, permanent link, and power cable.

Table A.6 describes network device information, while Table A.7 shows network equipment object information. Table A.8 shows permanent link object information, Table A.9 shows code object information and Table A.10 shows power cable object information.

Table A.6 — Network device information

Information	Description
Service ID	IDs that identify systems to which network devices belong.
Device ID	IDs that identify devices.
Port information	Information that reveals the number of ports, port numbers, whether there are routing and filtering functions and whether PoE power supply is available. When there are both HUB and routing functions, ensure that it is possible to confirm the functions of each port. When PoE power supply can only be made from limited ports, ensure that it is possible to identify from which ports electrical power can be supplied.
Supplier	Information that shows arrangements for shipyards, makers and ship owners.
Installation location	Information that identifies locations at which network devices are installed. Information that confirms that network devices are fitted inside and identifies the equipment inside the network devices, when network devices are fitted inside racks or boards.
Earth	Information that confirms whether network devices are earthed.
Note	Precautions to take when installing network devices.

Instruction manuals for installing network devices contain information on whether it is necessary to earth power sources and communication cables to which they shall be connected. When they shall be earthed, confirm whether network devices are installed where they can be earthed.

When optical cables in cable type are connected to network devices, confirm that places where tension members can be earthed are near terminals.

Confirm links between ports and connection nodes. For example, equipment for PoE power supply cannot be connected to ports that are not for PoE power supply. 16425-Network equipment that is not compatible with trunk ports cannot be connected to ports that are configured as trunk ports.

Confirm that the device ID and address in Table A.5 do not overlap with other network devices, wireless network devices or network equipment.

Confirm that there is no incoherence in the access port trunk port in Table A.5. It should be confirmed that the nodes to which trunk ports are connected are equipment compatible with IEEE 802.1Q:2018 (TAG VLANs).

Table A.7 — Network equipment object information

Information	Description
Service ID	IDs that identify systems to which network equipment belongs.
Equipment ID	IDs that identify equipment.
Port Information	Information that reveals the number of ports, port numbers and whether PoE power supply is available.
Supplier	Information that shows arrangements for shipyards, makers and ship owners.
Installation location	Information that identifies locations at which network equipment objects are installed. Information that confirms that network equipment objects are fitted inside and identifies the equipment inside the network devices, when network equipment objects are fitted inside racks or boards.
Earth	Information that confirms whether network equipment objects are earthed.
Note	Precautions to take when installing network equipment objects.

Instruction manuals for installing network devices contain information on whether it is necessary to earth power sources and communication cables to which they shall be connected. When they shall be earthed, confirm whether network equipment is installed where they can be earthed.

Confirm that equipment IDs in Table A.8, Table A.9 and Table A.10 do not overlap with other network devices, wireless network devices or network equipment.

Confirm whether the connections are made to meet the requirements in Table A.8, Table A.9 and Table A.10.

Table A.8 — Permanent link object information

Information	Description
Cable type	Information that identifies types of cables (e.g. serial cables, category cables and optical cables).
Cable ID	IDs that identify cables.
Shield	Information on whether there are shields.
Earth	Information for figuring out whether permanent link objects shall be earthed.
Supplier	Information that shows arrangements for shipyards, makers and ship owners.
Connect device	Information that identifies connection devices.
Connect port	Information that shows the port numbers of connection devices.
Connect method	Information that shows connection methods (e.g. directly to connection devices and via Modular Jack).
Note	Precautions to take when installing permanent link objects.

Table A.9 — Code object information

Information	Description
Cable type	Information that identifies types of cables (e.g. serial cables, category cables and optical cables).
Supplier	Information that shows arrangements for shipyards, makers and ship owners.
Connect device	Information that identifies connection devices.
Connect port	Information that reveals the port numbers of connection devices.
Connect method	Information that shows connection methods (e.g. directly to connection devices and via Modular Jack).
Note	Precautions to take when installing permanent link objects.

Table A.10 — Power cable object information

Information	Description
Supply power	Information that identifies whether the power supply is AC voltage or DC voltage.
Cable ID	IDs that identify cables.
Shield	Information on whether there are shields.
Earth	Information for figuring out whether permanent link objects shall be earthed.
Supplier	Information that shows arrangements for shipyards, makers and ship owners.
Connect device	Information that identifies connection devices.
Connect terminal No.	Information that identifies the terminal numbers of connection devices.
Connect method	Information that shows connection methods (e.g. directly to connection devices, with terminal blocks and with receptacles).
Note	Precautions to take when installing power cable objects.

Table A.11, Table A.12, Table A.13 and Table A.14 are based on network design documents.

Table A.11 — Network device item in a network design document

Fields	Description	Max. number
Network device detail		
Service ID	IDs for identifying shipboard systems and related to Service ID described in Terms of use. Single Service IDs can sometimes have more than one system detail.	1
Service Name	Names of shipboard systems.	1
Device ID	IDs for identifying wireless network devices.	1
Model ID	Model ID.	1
Serial No.	Serial numbers with which equipment is uniquely identified.	1
Date	Dates on which wireless network devices' firmware is updated.	1
Version	Versions of wireless network devices' firmware.	1
General		
Location	Locations where wireless network devices are located (e.g. ECR and electric rooms).	1
Environment requirements	Environmental requirements that wireless network devices authorize or comply with (e.g. IACS UR E10 and IEC 60945).	1
Security requirements	Security requirements that equipment authorizes or complies with (e.g. this document and IEC 63154).	1
Manufacture	Manufacturers of wireless network devices.	1
Mode/Reference	Describes whether redundancy configurations can be applied.	1
Occupancy rate	Occupancy rates of wireless network devices.	1
Power supply	Electricity supplying systems (e.g. DC24V external power supplies and PoE).	1
Power consumption	Consumption of power.	1
Software/configuration version information		
Type	Describes whether firmware or configuration files.	1
File name	The names of files that are saved externally are described when configuration files are selected in Type.	1
Version	Versions of firmware or configuration files.	1
Last update	Dates on which firmware or configuration files are updated.	1
Maintenance policy	How maintenance is provided (e.g. on-site, remote, periodic and occasional).	1

Table A.11 *(continued)*

Fields	Description	Max. number
Remote communication	Communication systems are described when maintenance connection is provided online (e.g. telnet, SSH, http and https).	1
Access control policy	Access control policies for information in equipment are described when connections can be made from outside (e.g. read, write and execution rights).	1
Account information		
No.	Serial number of accounts. Information on all is described when a single equipment has more than one account.	unlimited
User/roll Name	Names of users or roll accounts.	unlimited
ID	Information for identifying users or roll accounts.	unlimited
Authority	Information for authorizing users or roll accounts (e.g. authorization systems and passwords).	unlimited
VLAN Setting		
VLAN ID	VLAN ID	unlimited
VLAN Name	VLAN Name	unlimited
IP Address/mask	IP addresses and subnet masks are described when network devices are layer 3 switches or routers for routing among VLANs.	unlimited
Remark	Ranges covered by IP addresses used in VLANs and supplementary explanations on VLANs are described.	unlimited
Port Information		
Port No.	Port numbers of network devices.	unlimited
Metal/Opt.	Types of cables to be connected.	unlimited
Link Speed	Available link speeds. When automatic negotiation is accommodated, describe it as e.g. 10 MB/s, 100 MB/s and 1,000 MB/s (auto).	unlimited
Duplex mode	Duplex modes that ports accommodate are described (e.g. half, full and auto).	unlimited
Access VLAN ID	IDs of VLANs to be connected are described when Port VLANs are configured.	unlimited
Trunk ID	IDs of VLANs to be connected are described when IEEE 802.1Q-2018 (TAG VLAN) is configured.	unlimited
MAC address	Mac addresses are described when they are allotted to ports.	unlimited
Cable ID	IDs of cables to be connected to ports are described.	unlimited
Device/Equipment ID	Device IDs or Equipment IDs of equipment to be connected to ports are described.	unlimited
Port No.	Port numbers of network devices are described when equipment to be connected are network devices.	unlimited
Loop Detect		
Loop watch	If the loop detect function is equipped, it is described whether it is valid or invalid.	1
Enable Port	All port numbers that activate loop detects are described.	1
Recover timer	Amount of time until ports are automatically recovered are described.	1
Mode	Mode of Loop detect (e.g. STP, RSTP and Turbo Link).	1
SNMP Setting		
Version	Versions of SNMP (e.g. v1, v2, v2c and v3).	1
SNMP System name	Names of network devices of which SNMP managers are notified.	1
Trap address	IP addresses of managers that inform status changes.	1
Trap	Conditions for status changes are described.	1

Table A.11 *(continued)*

Fields	Description	Max. number
Trusted host	IP address of hosts that authorize connections when remote access is made.	1
IP address	IP address accessed from SNMP Manager.	1
Syslog server	Describes the IP Address of the Syslog Server when sending information to the Syslog Server.	1
NTP Server	Describes the IP Address of the NTP Server when obtaining the time from the NTP Server.	1
Time zone	Time zones that network devices handle.	1
SNMPv1/v2 Information		
Communication name (RW)	Passwords for obtaining information for RW (get/set) in SNMP v1, v2 and v2c.	1
Communication name (RO)	Passwords for obtaining information for RO (get) in SNMP v1, v2 and v2c.	1
SNMPv3 Information		
SNMP Authentication Type	Types of user-authorized protocols when SNMP v3 is used (e.g. MD5, SHA and DES).	1
No.	Serial numbers of SNMP-authorized users. Information on all is described when a single equipment has more than one SNMP user registered.	unlimited
User ID	IDs for identifying SNMP-authorized users.	unlimited
Password	Passwords for authorizing SNMP-authorized users.	unlimited
Trusted MIB tree	Numbers of MIB sub trees to which SNMP users are allowed to refer are described. MIB sub tree numbers are selected from numbers in MIB tree information and described.	unlimited
MIB tree information		
No.	Serial numbers of MIB sub trees. Information on all numbers is described when a single equipment has more than one MIB sub tree registered.	unlimited
MIB tree	OIDs of MIB sub trees that authorize uses are described (e.g. OID = 1.3.3.4).	unlimited

Table A.12 — Wireless network device item in a network design document

Fields	Description	Max. number
Wireless network device detail		
Service ID	IDs that identify shipboard systems and related to Service ID described in Terms of use; single Service IDs may sometimes have more than one system detail.	1
Service Name	Names of shipboard systems.	1
Device ID	IDs that identify wireless network device.	1
Model ID	Model ID	1
Serial No.	Serial numbers with which equipment are uniquely identified.	1
Date	Dates on which wireless network devices' firmware are updated	1
Version	Versions of wireless network devices' firmware.	1
General		
Location	Locations where wireless network devices are installed (e.g. ECR and electric rooms).	1
Environment requirements	Environmental requirements that wireless network devices authorize or comply with (e.g. IACS UR E10 and IEC 60945).	1